VISIONIAS
INSPIRING INNOVATION

CLASSROOM STUDY MATERIAL

Internal Security

PART 1

AHMEDABAD BENGALURU BHOPAL CHANDIGARH DELHI GUWAHATI HYDERABAD JAIPUR JODHPUR LUCKNOW PRAYAGRAJ PUNE RANCHI

CONTENTS

VISIONIAS
INSPIRING INNOVATION

Classroom Study Material

Internal Security

CHALLENGES TO INTERNAL SECURITY THROUGH COMMUNICATION NETWORK

CONTENTS

1. What is Communication Network

Communication network is the **interconnection of electronic gadgets and devices** that enable them to transmit information in the form of data, voice and videos. The network infrastructure includes hardware and software resources such as mobile, laptops, sensors, servers, web applications, satellites, SCADA, LAN, WAN, Optic fiber network etc. It provides the **communication path and services** between users, processes, applications, services and external networks/the internet.

In section 70 of IT Act 2000, **Critical Information Infrastructure (CII)** is defined as: "The computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety."

With the increasing convergence of communication technologies and shared Information systems in India, critical Sectors are becoming increasingly dependent on their CII. These CIIs are **interconnected, interdependent, complex and distributed** across various geographical locations. **Threats to CII,** ranging from terrorist attacks, through organized crimes, to espionage, malicious cyber activities etc., are following a far more aggressive growth trajectory. Any delay, distortion or disruption in the functioning of any one of these CIIs has the potential to quickly cascade across other CIIs with the potential to cause political, economic, social or national instability. Protection of CII and, hence, Critical infrastructure of the Nation is the one of the paramount concerns of the Government.

2. Role of Communication Network in Today's World

- **Critical Infrastructure** sectors use communication networks to perform not just auxiliary functions but also every vital function, be it human resource management, production, project management or business analytics.
  - It enables **voice and data communication, shrinking the time and space barriers.**
    - » The financial sector is increasingly using digital technologies like net banking, ATM networks etc. which are dependent on communication network. Any breach in the communication infrastructure of the banking sector could pose danger to the **financial stability of India.**
- It **connects infrastructure systems, subsystems and constituents** in such a manner that they have subsequently become highly interrelated and interdependent. For instance, the power sector is getting transformed into **Smart Grid** using communication networking technologies.
- Similarly, smart cities, smart agriculture etc. are heavily dependent on interconnected systems.
- Large industrial and manufacturing facilities also use automation and thus depend on information infrastructure.
- Also, the government is investing huge resources in **creation of e-governance infrastructure** such as National e-Governance Plan, Digital India, e-Kranti etc.
- Thus, the network infrastructure has become the **backbone of the entire critical infrastructure** and is **ubiquitous** in our lives.

2.1. Special Case – Communication Network in the Smart city

Communications play a very important role in smart city. Smart city can also be seen as a collection of entities (living and non-living) in an urban area which is **always connected, fully aware, auto-managed, self-secure, adaptive and well informed.** The growing footprint of ulra-high speed broadband networks, pervasive wireless networks, cloud computing , crowd sensing, and software-defined infrastructure connect smart/mobile devices to generate relevant city data on a massive scale.

Communication drives every aspect of a smart city, from relaying the position of traffic, to transferring data on air quality, to providing citizens with remote services through apps or their computers. Communications infrastructure networks allow the city to create the city of the future.

The Communication Network for Indian smart cities include-

- Wired network – optical fiber networks
- Wireless networks – 4G, 5G, Wi-Fi
- Satellite network
- Machine-to-Machine connectivity
- Networks including MAN, WAN, PAN, HAN
- Dedicated resources that could be allocated for critical communication or communication during emergencies or disasters.
- Data gathered from smart devices and sensors across the city

- Smart Software to create valuable information and digitally enhanced services such as healthcare, safety and security, real time traffic monitoring, managing the environment, etc. shared across wired and wireless network

3. Types of threats to Communication Networks

As the price of failure of communication network is too high, they are the potential soft targets for disruption. Threats to network infrastructure can be broadly classified into two categories: natural threats and human induced threats.

3.1. Natural Threats

Natural threats encompass **floods, earthquake, tsunami, volcanic activities,** etc. These natural disasters could physically damage communication network.

For instance, in an **ICT driven smart city,** if a minor earthquake snaps local telecommunication towers, it will disrupt all the ICT dependent utility services such as power, water supply etc. The local ATMs and banking services might stop functioning.

Similarly, **solar storms** might damage communication satellites orbiting earth which will affect all the sectors dependent on satellite communications such as weather forecasting, mobile services, DTH, tele-medicine etc.

3.2. Human induced threats

Various actors may work as a threat to Communication network such as-

- **Various actors** may work as a threat to communication networks such as-
  - Insiders in the form of disgruntled employees or compromised/socially engineered employees.
  - Economic, military or adversary nation states.
  - Criminal syndicates to terrorist outfits.
- **Types of threats-** This includes all the attempts made by malicious actors to gain access to the system with the intent of causing harm or damage. The threat actors **exploit the underlying vulnerabilities** within the application software, control systems software, hardware or even the people to get access to the desired location in the network.
- Once the network is breached, they can execute commands, steal sensitive information such as design or configuration or corrupt the information flowing to the interfaces.
- All of actors have different capacities and capabilities. A nation state has the technological means and the requisite wherewithal to conduct and sustain long-term operations, which include espionage, data or credentials theft and execution and monitoring of attacks.
- The terrorist organizations are also alleged to be capable of perpetrating attacks on CII, with the ease of access to the professional skills available in the market.
- The following are **possible targets** in a network operation infrastructure-
  - The devices in form of routers, switches, firewalls, mobile phones, database and domain name system (DNS) servers;
  - Web portals, protocols, the ports and communication channels;
  - Satellite network communication systems;

- Network applications such as cloud-based services;

The major security threats to communication network can take the following forms:

- Destabilising critical infrastructure like Nuclear power plants, share market operations through cyber-attacks, etc. For example, Stuxnet's alleged involvement in destabilising Iran's Nuclear programme.
- Intellectual property right infringement through digital privacy.
- Data alteration and data destruction on the website and impairing its operations, especially in the case of government websites.
- Information warfare.
- Economic threats like theft of banking data such as customer's credit and debit card data, frauds, etc.

3.2.1. Classification of Human Threat Actors

Though, there is no clear distinction between the human threat actors, but they can be broadly classified as follows-

- **Terrorists and Non-State Actors**
  - The primary objective of a terror outfit generally is **to instigate terror in the minds** of the victims as well as the onlookers. An attack on communication network – **physical or cyber-** would have crippling effects and far-reaching impact on the victims and the **psychology** of the witnesses, thus fulfilling the objective of terrorists.
  - With the growing radicalization among the educated youth, these terror outfits have access to the human resources possessing good working knowledge of computers, networks and programming. As a matter of fact, some of the groups such as the Islamic State of Iraq and Syria **(ISIS) and Lashkar-e-Taiba** are known to have developed their own secure communication applications for smartphones.
  - Even more, with the **support of the adversarial states,** terror groups have become a more credible threat as they are equipped with enough financial resources and access to technology and skills.
  - In addition to terror outfits, cyber criminals are also direct threat to critical information infrastructure (CII). Their

States Acquiring Offensive Cyber Capabilities

Several countries have established institutions to develop offensive cyber capabilities.

- **United States** has raised US Cyber Command (USCYBERCOMM) for offensive capabilities.
- **South Korea** created a Cyber Warfare Command in 2009. This was also in response to North Korea's creation of cyber warfare units.
- The **British Government** Communications Headquarters (GCHQ) has begun preparing a cyber force, as also France.
- The **Russians** have actively been pursuing cyber warfare.
- In 2010 **China** overtly introduced its first department dedicated to defensive cyber warfare and information security in response to the creation of USCYBERCOM. The race is thus on across the world.

Examples of Terrorist Attacks and Crippling Effects

- 9/11 attack on the World Trade Center directly affected banking and finance, telecommunications, emergency services, air and rail transportation and energy and water supply.
- Attacks on the urban transit systems in London and Mumbai.

prime driver is monetary gains that can be easily leveraged by any adversary – terror group or nation state.

- Non-state actors have disabled critical infrastructures by using cyber-attacks, drones to smuggle narcotics, arms and ammunitions across borders
- Dark web, AI-enabled tools and software have been widely used to create fake news, recruit members through online radicalization etc.
- Non-state actors can transfer money through virtual currencies and indulge in money laundering, drug trafficking etc. E.g. 'Wannacry' ransomware attack in 2017.

Nation States

- Nation states are the **most potent threat** to information infrastructure in terms of resources at their disposal. In the absence of globally agreed upon norms or legal measures to dissuade nation states from targeting each other's CII in the face of any eventuality, the CII remains a lucrative target. Under such circumstances, cyber-based attacks have the potential to amount to an act of warfare as they might be utilized to destabilize a nation state.
- Lately, **advanced persistent threats (APTs)** have wholly transformed the threat landscape. These are the **state – sponsored campaigns targeted against Critical information infrastructure,** especially communication network. APTs are **sophisticated, targeted and prolonged** attempts of intrusion and information theft using a **wide variety of techniques,** including SQL injection, malware, spyware, phishing and spam.
- Attacks led by the APTs **infiltrate into sensitive systems,** such as email servers, and they are designed to remain **undetected or hidden** from the administrators— sometimes for years. Since APTs are **highly advanced, planned and executed meticulously,** they hardly leave any trace, and therefore render traditional means of security and forensics incapacitated. The APTs can be used for the disruption of industrial operations or even destruction of industrial equipment.

3.3. Examples of security threats to the communication networks

Network and Packet sniffing

Smaller packet bundles of large information are picked and processed by applications through **"off-network".** This kind of application that interprets the network packets is called packet sniffers. This poses a grave threat to government and business data flow.

Denial of services (DoS)

This is the most infamous attack among attacks on communication networks and most difficult to eliminate. The ease of attack and potentiality of damages make them an important threat that deserves special attention. Distributed denial of services attack refers to a simultaneous attack on many systems which temporarily brings down the targeted website/system.

IP spoofing

IP spoofing is an attack from an attacker outside the targeted network by pretending to be a trusted computer. It can use the IP address of the targeted network or an authorized and trusted IP address

Man-in-the-middle attacks

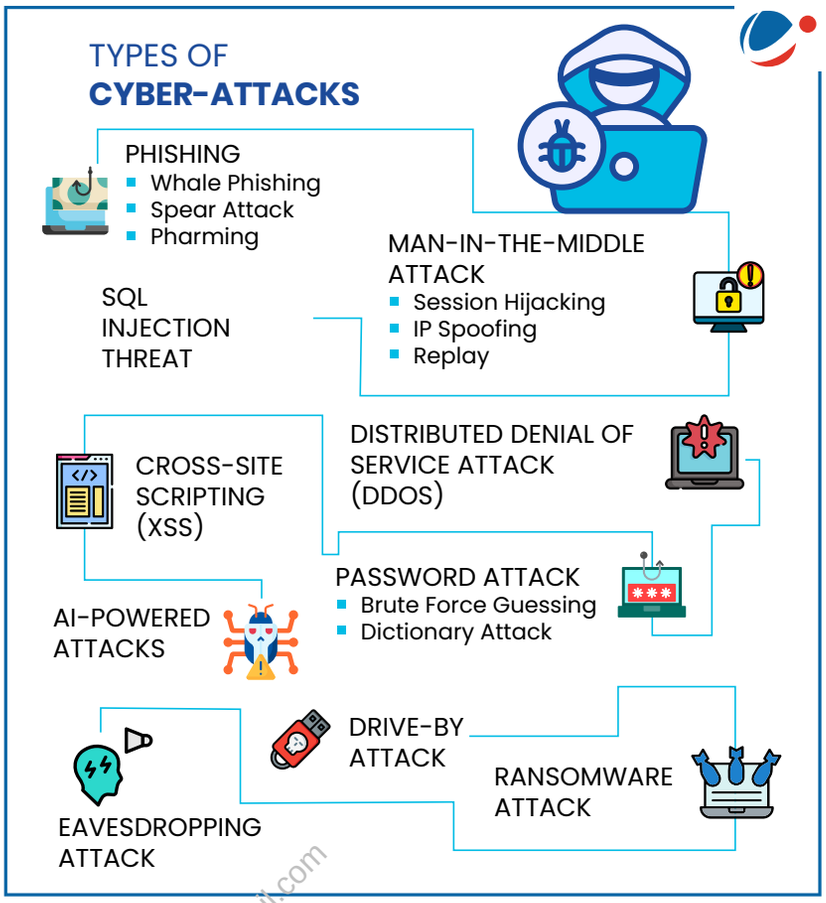
It refers to access to network packets coming across networks. It implements network sniffers and routing and transport protocols to do data theft, gaining access to the system's internal network resources, Denial of service, the introduction of new information in existing networks to

Virus or Trojan Horse attacks

Viruses and trojan horse applications are a threat to end-user computers. Viruses are malicious software attached to a programme to execute a directed, unwanted task on the user's workstation. Trojan horse is an application disguised to hide the original identity of attack tools. It not only attacks the user system but also spreads through engaging in automatic spread to known systems.

Ransomware

It is a type of malware that restricts access to certain information from the actual owner to demand a ransom paid to the creator of malware. They use encryption, locking the system to deny user access to important information. A recent instance was the attack by WannaCry ransomware.



4. Importance of Securing Communication Networks

- The communication networks **form the basis of digital ecosystem.** For ensuring **overall cyber security,** it is imperative to secure communication networks from all types of possible threats – human as well as natural.

Case of Estonia

Estonia is one of the most densely connected countries and has pioneered facilities such as e-government, Internet voting and online banking transactions (98 percent). In 2007, it witnessed a massive Internet traffic, which brought down the networks of its banks, broadcasters, police, parliament and ministries. The scale and timing of this attack targeted at the core of its information infrastructure. It practically brought Estonia to a standstill.

- **National Security:** Disruption of communication networks can disturb stability of country especially if communication networks supporting critical sector are targeted. The failure of communication network has potential to **cripple security agencies,** rendering them ineffective. This can be understood by following-
  - Security agencies follow **hierarchy** and have certain **chain of commands.** For exchange of information such as intelligence– both horizontally and vertically, the security forces and agencies use communication technologies such as wireless handsets. The working of these devices requires robust communication network infrastructure. The attacks on such communication infrastructure could have far reaching implication on capabilities of securities agencies.
  - The **gathered intelligence** by local intelligence officer cannot be communicated to competent decision-making authorities in wake of such failure. The resulting delay in decision making would prevent forces and authorities taking timely corrective actions.
- **Growing Inter-dependencies:** All the critical sectors, such as transportation, communications and government services, depend upon the power/electricity sector for their basic requirement of electricity supply, which in turn powers the railways, airports and communication systems such as switching centres or telephone exchanges. In an **interdependent** system, the power/electricity sector itself depends on transportation for fuel supplies and communications for its data transmission or to maintain the health of the transmission/distribution networks.
- **Protecting Digital Sovereignty:** From individual's perspective, digital sovereignty is all about exercising control and authority by internet users to decide freely and independently which data can be **gathered, distributed, used and saved** about them. Since all the data flows over the communication networks, digital sovereignty of people would get compromised if communication networks are not secured properly.
- **Building Confidence on Digital Technology:** Internet is penetrating all aspects of our lives and the government also is encouraging its people to use digital services such **Digi-Locker** for storing important documents. For people to use these services and participate in such initiative, it is imperative to secure such communication networks so as to build confidence and trust of people on digital technology.

Security Requirements, Threats, and Attacks

Requirements

Confidentiality	Integrity	Availability	Non-Repudiation
Unauthorized Access to Information	Unauthorized Modification or Theft of Information	Denial of Service or Prevention of Authorized Access	Accountability; Denial of Action that took place, or Claim of Action that did not take place

Threats

Attacks

Listening	Interactions	Planted in System	After-the-Fact
Eavesdropping	Masquerade	Virus Worms	Denial of Action
Traffic Analysis	Bypassing Controls	Trojan Horse	Claim of Action
EM/RF Interception	Authorization Violation	Trapdoor	Stolen/Altered
Indiscretions by Personnel	Physical Intrusion	Service Spoofing	Repudiation
Media Scavenging	Man-in-the-Middle		
	Integrity Violation		
	Theft		
	Replay		

Modification	Denial of Service
Intercept/Alter	Resource Exhaustion
Repudiation	Equipment Failure
	Software Failure

5. Challenges in Securing Communication Network

The process of protecting communication networks has many challenges; some of them are discussed below:

- **External sourcing of equipment and technology:** Much of the software and hardware that makes up communication system is imported from other countries (Chinese devices account for more than 60% of total telecom equipment imports). These devices may contain a **back-window for transmitting information.** Recently, Indian Electrical and Electronics Manufacturers Association **(IEEMA)** highlighted the concern of **"security threat" in critical power infrastructure** with increased use of foreign automation and communication systems in operation and management of the electricity grid. The malware and spyware in these communication devices can be activated any time, even from a remote location.
- **Evolving nature of threats:** A rapid pace of technology evolution means continuous evolution of threats to security systems. This leads to constantly evolving security systems to thwart such attacks, which becomes a tedious work as attackers can have the **privilege of anonymity and a wide choice** available as their target system.
- **Involvement of state and non-state actors:** The present-day threats are **ambiguous, uncertain and indistinct** in terms of their identity and goals. While nation states have broader political or security motivation, motivation of malicious non-state actors is hard to comprehend, and could be anything from monetary gain to terrorism or even a narrow political agenda.
- **Inadequate understanding of inter-dependencies:** This is one of the reasons for critical infrastructure being so complex. The **lack of scientific analysis and tools** for comprehending inter and intra-sector dependencies is the primary reason for the poor preparedness of our security agencies.
- **Structural Challenges:** India faces structural challenges as there is no clear demarcation of powers between Union and states along with a multiplicity of security agencies.
    - **Federalism-** Cyber space transcends geographical boundaries and spread across the country. Cyber security as a subject is not specifically listed in any of the three lists in **7th Schedule.** Due to this, sometimes Central Government faces challenges from state governments in the form of their opposition to its several initiatives. The state governments' major concern relates to the preserving federal polity of India. For instance, when **NATGRID** was setup as an **integrated intelligence master database structure** for counter-terrorism purpose connecting databases of various core security agencies under the Government of India, it was opposed by state governments.
    - **Coordination among security agencies:** Various departments and ministries of the government and private sector associations have set up cyber security agencies, which are more aligned to serve their own mandates and interests. This **fragmented approach** poses a substantial challenge, as most of these agencies **work in silos** and devise policies according to the small set of stakeholders.
    - **Lack of a national security architecture** that can assess the nature of cyber threats and respond to them effectively.
- **Private sector owns and operates a significant part of the information infrastructure** such as telecom, banking, stock exchanges, energy utilities etc. They see measures such as security auditing and regulations as addition to their operating costs.
    - The government **cannot leave it to the private sector alone** for securing its own CII. For example, if there is a cyber-attack on one of our national stock exchanges, it could bring down trading operations, impacting the economy and creating panic among investors.

- **Lack of incentives to improve Cybersecurity:** The actual expenses from the recent and high-profile breaches at firms like Sony,Target and Home depot,etc amount to less than 1%of the annual revenues, which after reimbursements from the insurance companies turns out even less. The absence of beneficial market incentives may help explain why private firms often fail to invest in even relatively low-cost security measures.
- **Poor enforcement of regulations-** Private sector views **regulatory control** as an impediment in their organizational objectives, which primarily revolves around creation of wealth for the shareholders. Therefore, many firms that operate critical infrastructure tend to under invest in cyber-defence. They deliberately search for loopholes in regulations and bypass them for cutting their cost of operation. Also, **lack of testing capacity** with government agencies allows network operators to procure cheaper but vulnerable communication equipment.

6. Building a Risk Management Strategy

6.1. Understanding Risk

Risk is defined as "the potential that a given threat will exploit vulnerabilities of an asset and thereby cause harm to the organization". From this definition, it is illustrated that risk is a function of

- The likelihood of a given **Threat Event.**
- Exercising a particular "potential" **Vulnerability** of an asset.
- With resulting **Consequences** that impact operation of the asset.

The **Threat Event** actually consists of components that all can significantly impact risk, including:

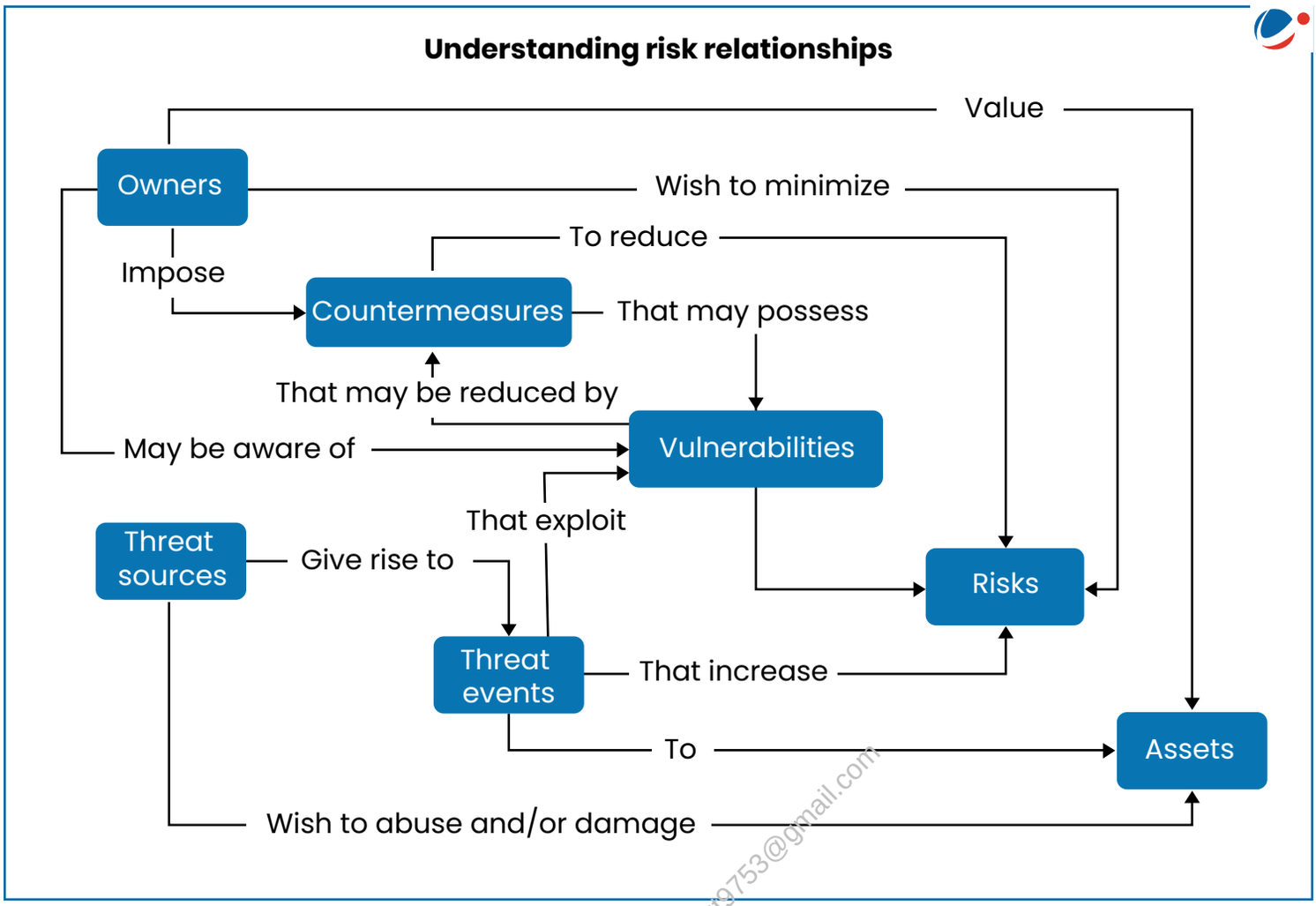
- Threat Source or Actor to carry out the event.
- Threat Vector to initiate the event.
- Threat Target which the event attacks.

When identifying risks, the organisation must start by understanding threats, vulnerabilities, and the consequences of their convergence.

Threats are circumstances or events with the potential to negatively affect an organization's operations or assets through the unauthorized access of information systems. Threats can manifest everywhere—in the form of hostile attacks, human errors, structural or configuration failures, and even natural disasters.

Vulnerabilities can be defined as weaknesses in an information system, security procedure, internal control, or implementation that can be exploited by a threat source. Often the result of inadequate internal functions like security, vulnerabilities can also be found externally in supply chains or vendor relationships.

Consequences can best be defined as the adverse results that occur when threats exploit vulnerabilities. Their impact measures the severity of consequences, and your organization will need to estimate such costs when attempting to assess risk. Keep in mind these costs usually come in the form of lost or destroyed information, which can be a significant business setback for any organization.



6.2. Need for a Risk Management Strategy

- **Mitigating cyber risks and preventing attacks–** Implementing a cyber risk management strategy helps to identify the threats to an organisation. Developing a risk treatment plan also helps to address the risks and put the correct defences in place. This reduces the threats from cyber-attacks.
- **Reducing costs and protecting revenue–** Many attackers motive is financial gain. This means any organisation can be affected. It is important to minimise the risk of falling victim to an attack and mitigate the loss of revenue you could lose. Complying with certain regulations as part of the cyber risk strategy will help organisation's avoid hefty fines that can be given for non-compliance.
- **Increased organisation's reputation–** Proving to your clients and customers that you take cyber security seriously gives your organisation a competitive edge. Organisations who prioritise their customer's or client's data, gain their trust; resulting in loyalty and increased long-term business success.
- As more of our physical world is connected to and controlled by the virtual world, and more of our business and personal information goes digital, the risks become increasingly daunting.
- Risk management is a key requirement of many information security standards and frameworks, as well as international laws such as the GDPR (General Data Protection Regulation).

6.3. Building an Effective Risk Management Strategy

The constituents of an effective risk management strategy include:

1. **Risk Assessment:** The process of **identifying and reviewing** the risks that you face is known as risk assessment.

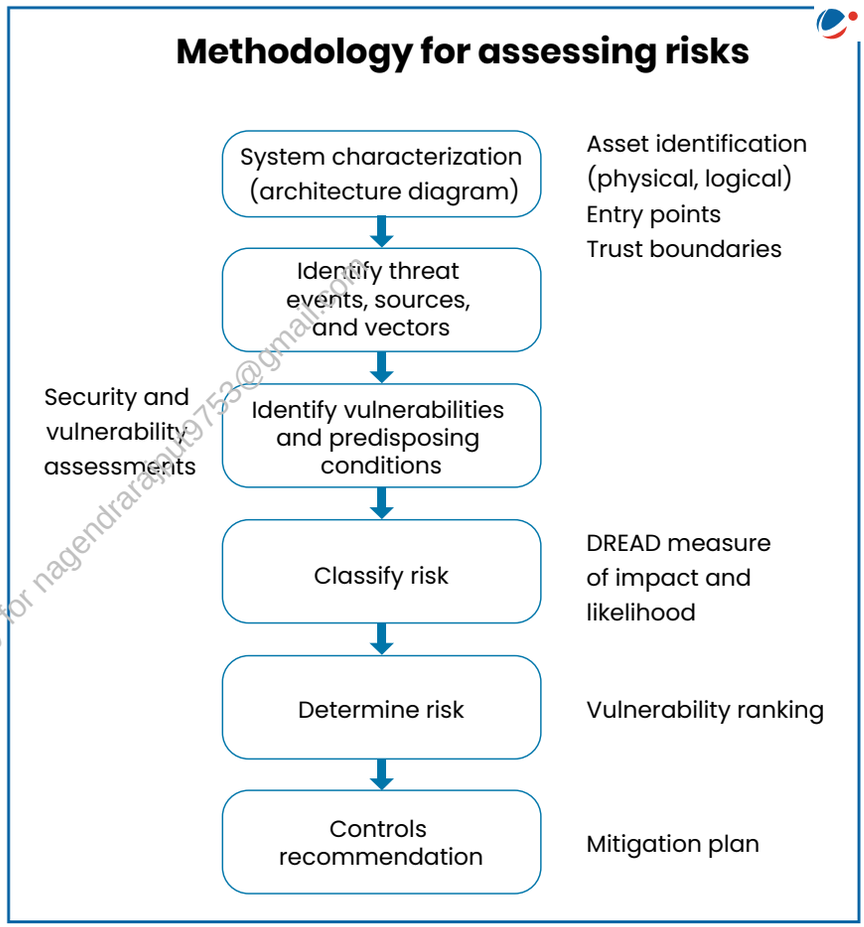
   By assessing risks, you are able to be actively aware of where uncertainty surrounding events or outcomes exists and identifying steps that can be taken to protect the organisation, people and assets concerned.

   A comprehensive security assessment includes data risks, analysis of database security issues, the potential for data breaches, network, and physical vulnerabilities.

2. **Risk reduction / Risk Mitigation Measures:** Technological risk mitigation measures include encryption, firewalls, threat hunting software, and engaging automation for increased system efficiency.

The best practices in risk mitigation include:

- Conduct cybersecurity training programs.
- Deploy multi-factor access authentication.
- Deploy dynamic data backup.
- Automatically update software periodically.



3. **Residual cybersecurity risk:** This is the risk left over after applying all mitigation measures—the type of unavoidable risk the organisation can't do much about. There are two choices for residual risk—

- Learn to live with it or
- Cybersecurity insurance provides a last-ditch option for lessening residual risk and stands to become more popular as the damage cost of cyber incidents becomes easier to calculate.

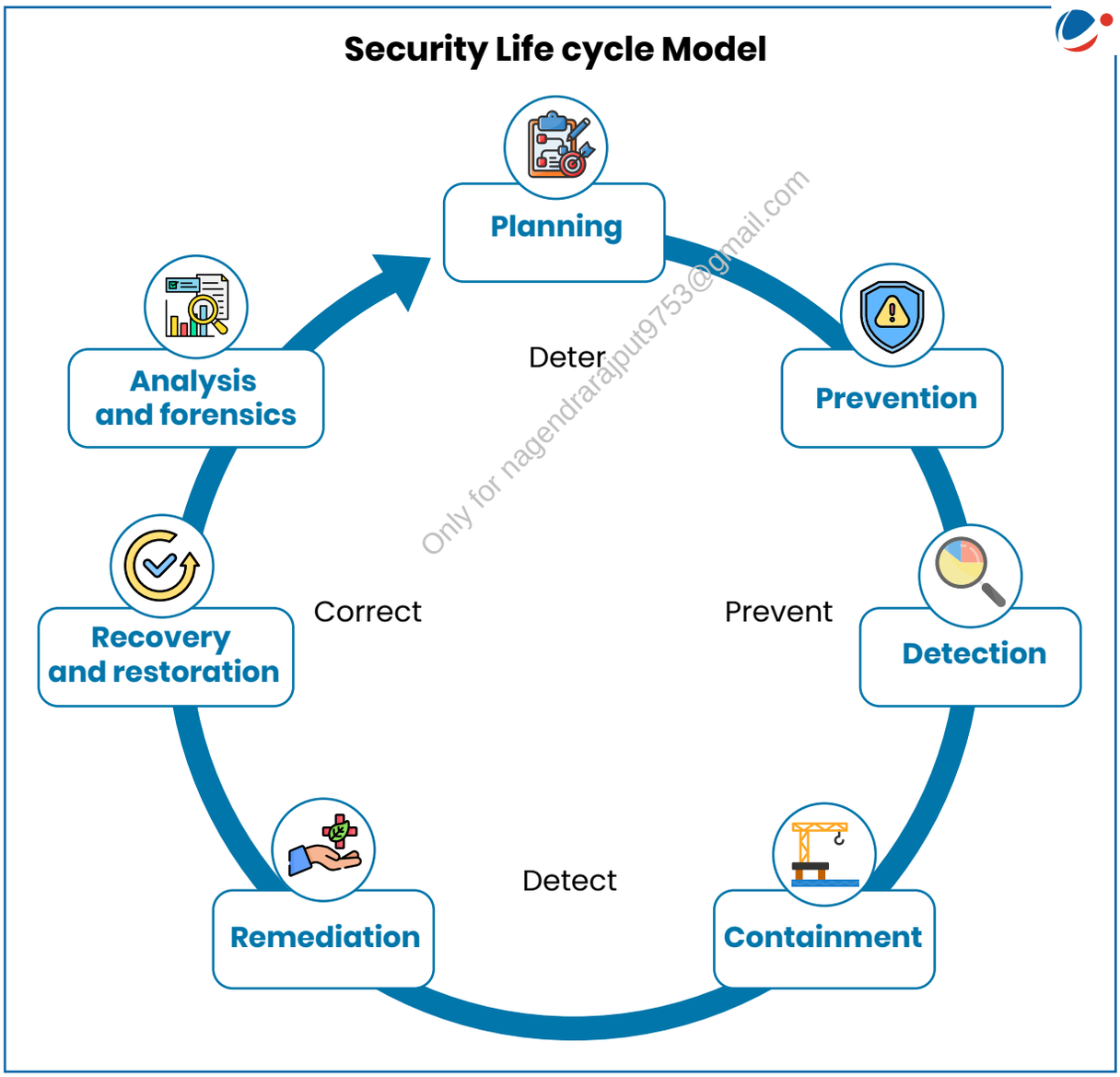
4. **Ongoing Monitoring:** After identifying, assessing and mitigating risks in the communication network, it is needed that the organisation ensures constant monitoring of the envrironment so that internal controls maintain alignment with IT risk. The organization will need to monitor:

- Regulatory change- Staying abreast of all regulations and their shifts will ensure your internal controls align with outside expectations.
- Vendor risk- Be sure to assess and document security and compliance controls as new vendors onboard. The vulnerablities of the vendors can pose a security risk to the organisation.
- Internal IT usage- Need to constantly update the technology the internal teams use and how they use it to stay ahead of potential gaps.

Other best practices in the risk management process can be summarised as:

- Implement technology solutions to detect and eradicate threats before data is compromised.
- Establish a security office with accountability.
- Ensure compliance with security policies.
- Make data analysis a collaborative effort between various stakeholders.
- Ensure alerts and reporting are meaningful and effectively routed.

Conducting a complete IT security assessment and managing enterprise risk is essential to identify vulnerability issues. Development of a comprehensive approach to information security is the need of the hour.



7. Recent Developments

7.1. WannaCry Malware

WannaCry virus was a **cryptoransomware,** also known as **WannaCrypt,** which affected thousands of computers spread over 150 countries. The WanaCrypt0r 2.0 bug encrypted data on a computer within seconds and displayed a message asking the user to pay a ransom of $ 300 in Bitcoins to restore access to the device and the data inside

Who was behind the attack and their motivation?

- it is widely accepted that the hackers used the 'Eternal Blue Hacking Weapon' created by America's National Security Agency (NSA) to gain access to Microsoft Windows computers used by terrorist outfits and enemy states.
- Since over a thousand computers in the Russian Interior Ministry, as well as computers in China, were hit, some of the state- or quasi-state actors suspected of carrying out large scale break-ins of computer systems in the United States will, on this occasion, start as not being suspects

Vulnerability of Indian Databases like Aadhar

- The attack was specifically targeted at Microsoft Windows devices. Microsoft claims it "released a security update which addresses the vulnerability that these attacks are exploiting", and advised users to update their systems in order to deploy the latest patches.
- However, in India, where most official computers run Windows, regular updates might not be a habit, and hence the vulnerability could be very high.
- Since the user's bank account is linked with his Aadhaar number, the ransomware can potentially lock down the account and make it unusable unless a ransom is paid.

Approach to tackle the vulnerabilities of the digital Age

The need for a four-phase approach to cybersecurity:

- **Predict** by performing an exposure analysis;
- **Prevent** by deploying a defensive solution to reduce the attack surface;
- **Respond** by determining how a breach happened and what impact it had on systems; and
- **Detected** by monitoring infrastructure for signs of intrusion or suspicious behaviour.

The least one can do is stop clicking links that you don't trust, and stop downloading software from unknown sources.

7.2. Hybrid Warfare

Hybrid Warfare entails an interplay or fusion of conventional as well as unconventional instruments of power and tools of subversion

As early as 1999, **Unrestricted Warfare,** a publication by China's People's Liberation Army, mapped the contours of hybrid warfare, a shift in the arena of violence from military to political, economic and

technological. The new weapons in this war were those closely linked to the lives of the common people. It involves the collection of non-harmful granular information about individuals that is put together in a broader framework for deliberate tactical maneuvering in the future.

Recent case of Chinese firms

- Recently, the Chinese-only website of **Zhenhua Data Information Technology Co,** was pulled down after it was caught **targeting individuals and institutions** in politics, government, business, technology, media, and civil society.
- Claiming to work with Chinese intelligence, military and security agencies, Zhenhua monitors the **subject's digital footprint** across social media platforms, maintains an **"information library,"** which includes content not just from news sources, forums, but also from papers, patents, bidding documents, even positions of recruitment.

Key Domains of Hybrid Warfare

- **Political warfare:** Interference in the political activities of the countries to their detriment.
- **Technological warfare:** Using technological capabilities to inflict harm on entities.
- **Military Warfare:** Action such as use of improvised explosive, guerrilla warfare, etc.
- **Economic Warfare:** To weaken the economy by disrupting the supply chains, introducing counterfeit currency, etc.
- **Social warfare:** Exploiting already prevalent social issues and vulnerabilities via propaganda,etc

- Significantly, it builds a **"relational database",** which records and describes associations between individuals, institutions, and information. Collecting such massive data and weaving in public or sentiment analysis around these targets, Zhenhua offers **"threat intelligence services."**

Does this flout any of India's Laws?

- Under the **Information Technology Rules, 2011, under the IT Act, 2000,** personal data is "any information regarding a natural person, which either directly or indirectly, in combination with other information available or likely to be available... is capable of identifying such person." This, however, does not include information available freely or accessible in the public domain.
- However, as per the new data protection legislation, collection of information by a third party source and sharing it with rival country's intelligence, without consent of the user will be illegal.
- However, enforcement of privacy laws in a foreign jurisdiction is almost impossible because they differ from one country to another.

Threats posed

- Through targeted cyberattacks, disinformation campaigns and espionage, hybrid warfare seeks to incite social discord, disrupt economic activities, undermine institutions, and discredit political leadership and the intelligentsia.
- This may include attacks on critical infrastructure like power grids, business systems, and defence systems.
- The information may be used to plant disharmony

Associated challenges for India

- **Encourages new forms of terrorism** such as **Lone wolf attacks, hybrid militants,** creation of **sleeper cell** that are difficult to detect.
- **Cyber-attacks:**
  - Privacy and personal data theft
  - Insecure framework of **mobile apps**
  - **Cyber espionage** issue with China and Pakistan
- **Interference in electoral processes** through media and social media campaign.
- **Using disinformation** and **fake news** to create a **parallel reality** and fuel **social fragmentation.**
- **Financial influences** through investments like in unfavourable energy-supply deals.

and communal tensions within a society which is eventually a threat to the unity of the country.

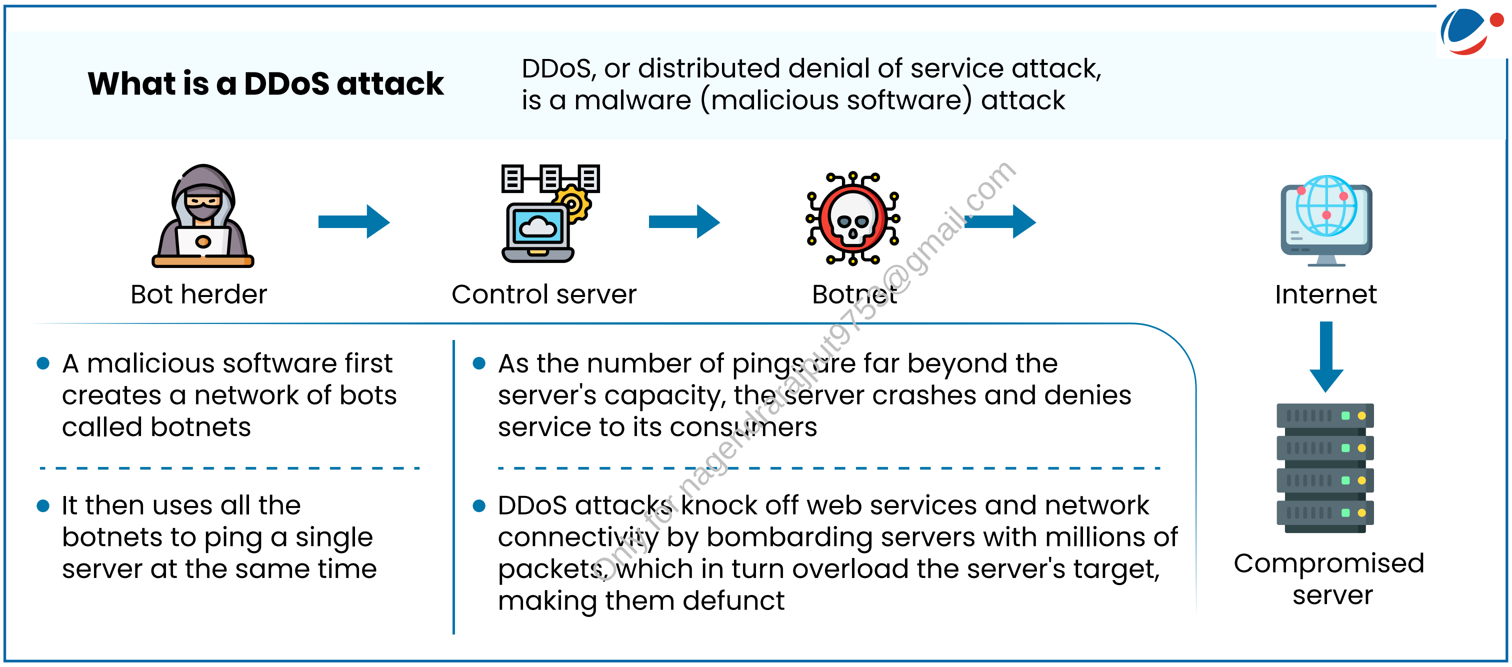
Other recent attacks and the emerging trends

- Recently, the Central Bureau of Investigation (CBI) has sent alerts to all the States, Union Territories and the central agencies on a malicious software (cerberus) threat that is taking advantage of the Covid-19 pandemic. The banking trojan known as Cerberus takes advantage of the COVID-19 pandemic and sends SMS to lure a user into downloading the link containing the malicious software.

About Pegasus

- It is a spyware developed by an Israeli Cyber Arms firm.
- It mainly uses exploit links, clicing in which installs Pegasus on the target's phone
- It exploited zero-day vulnerabilites in in he phone's operating sytems (OS) to attain all user access of the phone.
- In case of Whatsapp, a specially crafted call was used to trigger a buffer overflow, which int turn was used to take control of the device.

- The recent digital security breach by a spyware called **Pegasus** compromised phones of multiple activists, journalists and lawyers in India. The spyware was able to track multiple user applications like messages, emails, audio calls, browser history, contacts including end-to-end encrypted data.



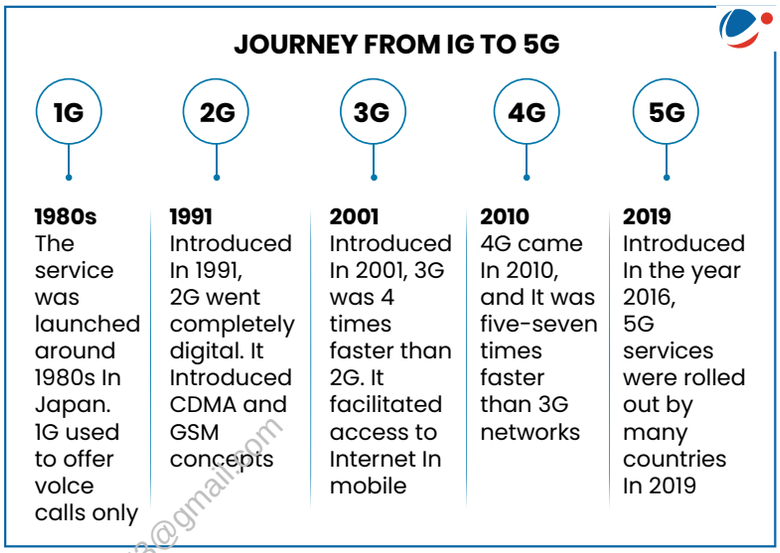
- A German Security firm, **Greenbone Sustainable Resilience** published reports about medical details of over 120 million Indian patients being leaked and made freely available on the Internet.
- A new malware Saposhi, which is capable of taking over electronic devices and turning them into **'bots'** which can be used for any purpose, including a Distributed **Denial of Service attacks** which can cripple entire industries.
- **Recent emerging trends include:**
- Ransomware:
  - Initially, ransomware attacks followed a pattern akin to fire and forget, that is, it was used for small scale extortion from individuals. Now, however, the pattern has shifted to more focused and targeted attacks for larger returns like targeting the server of an organisation. The effect is to turn entire organisations into victims rather than individual users, and the pay-off for the extra effort involved in performing this kind of an attack is often huge.

- Rise in the number of cases of Social Engineering Attacks
  - Social engineering attack involves manipulating people into breaking normal security procedures and best practices in order to gain access to systems, networks or physical locations, or for financial gain. It relies heavily on human interaction.
  - Recently the **Ministry of Home Affairs** asked officials to avoid unsolicited calls, visits or email messages from unknown persons claiming to represent some organisation, to prevent the leak of sensitive information.

7.3. 5G and Internal Security

India's 5G journey started in August 2018, when TRAI issued recommendations on the auction of 5G spectrum bands. 5G is a wireless communication technology launched in India in 2022. It is the next generation mobile networks technology after 4G LTE networks. The 4G networks were capable of achieving the peak download speed of one gigabit per second. With 5G the speed could be increased upto 10Gbps.

- India ranks 14th globally in 5G speeds with 301.86 Mbps in Q4 2023.
- 5G availability in India rose from 28.1% in Q1 2023 to 52.0% in Q4 2023.



Security risks posed include:

- A report prepared by security agencies has pointed out that 5G networks have 200 times more attack vectors, or paths to gain access to a network, compared to their 4G predecessors.
- This network would move away from centralized, hardware-based switching to distributed, software-defined digital routing. As the 5G is based on virtualised networks, it would require robust protocols for security.
- It uses common language of Internet Protocols and well-known operating systems, hence vulnerable.
- It is using early generation of AI and that itself can be vulnerable. An attacker that gains control of the software managing the networks can also control the entire network. Due to shared infrastructure of 5G, it has potential for mass failure across multiple linked-networks resulting in the paralysis of the core infrastructure when any of the linked-networks is successfully attacked.
- The dramatic expansion of bandwidth itself makes 5G more vulnerable.

Technical specifications for 5G

- High data rates (1 Gbps for hotspots, 100 Mbps download and 50 Mbps upload for wide-area coverage)
- Massive connectivity (1 million connections per square kilometre)
- Ultra-low latency (1 millisecond)
- High reliability (99.999% for mission critical 'ultra-reliable' communications), and
- Mobility at high speeds (up to 500 km/h i.e. high-speed trains).

- 5G networks are vulnerable to mobile network mapping, or MNmap, attacks. Using actual devices and

networks, it can gather the information sent by the devices in plain text and create a map of devices connected to that network.

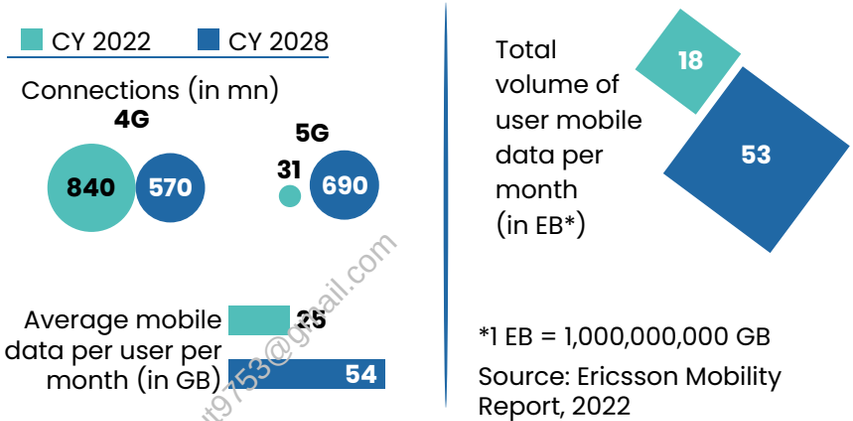
- Besides, there are supply chain security issues with platforms purchased from overseas with backdoor vulnerabilities purposely built into mobile carrier network and equipment.
- Broadly, the 5G poses a higher security threat as there are more vectors through which hackers and adversaries can attack. Moreover, as the critical emergency services for smart cities and industries would be based on 5G technology, any interference with the 5G network enabling such services would be catastrophic.

Suggestions

- 5G would produce massive data and this demands special efforts for its protection. There is a need for comprehensive system for data storage, processing and sharing to be put in place. The centrality of having servers placed in India cannot be underestimated.
- Need to use indigenous equipment and software for the complete roll out of 5G in India.
- The security of the 5G network should be the shared responsibility. The different stakeholders and operators must understand their roles for the security of the entire network and should act as a joint unit in this direction. It is important for companies and operators dealing with storage, transmission, processing and analysis of data to align and collaborate for end to end security.

The rise of 5G usage in India

The adoption of 5G, while happening at a faster pace, does not mean the end of 4G. However, it does mean that we'll use more data on our phones.



- Special attention would have to be paid by mobile network operators who must adopt a continual risk-based approach to monitoring their network and services, evolving their security controls around emerging threats. Edge computing creates a larger surface for sophisticated attacks and this demands users to strictly comply with basic security fundamentals.

7.4. Steps taken by the Government

India has elevated its response to protect communication infrastructure in the recent years.

- The legal framework to address the threats emanating from cyberspace to it, especially from cyber terrorism, was developed in the amendment made in 2008 to the IT Act, 2000.
- The government launched National Telecom Policy of 2012 where it has set a target for domestic production of telecom equipment to meet the Indian telecom sector's demand to the extent of 60 to 80 per cent by 2020.
- The **National Telecom Policy 2018** stresses on developing robust digital communications network security frameworks and aims to ensure digital sovereignty to be achieved by 2022. Some key features pertaining to security of communication networks include:

- To establish a comprehensive data protection regime for digital communications that safeguards the privacy, autonomy and choice of individuals.
- Enforce accountability through institutional mechanisms to assure citizens of safe and secure digital communications infrastructure and services.

- The **National Digital Communications Policy, 2018** also stresses on making a robust communication infrastructure which is ubiquitous, resilient, secure and affordable.
- The **Computer Emergency Response Team (CERT),** at both the national and State-levels, have been told to respond aggressively to cybersecurity attacks for malicious attacks like stealing of sensitive data, etc.
- To ensure that imported communication equipment are free from vulnerabilities, a number of measures, such as making **local certification mandatory,** have been announced. They include setting up of equipment testing laboratory.
- **Cyber Swachhta Kendra** (Botnet Cleaning and Malware Analysis Centre) has been launched for providing detection of malicious programmes and free tools to remove such programmes.
- The **Ministry of Communications and Information Technology** has also repeatedly urged the Telecom companies to take note of vulnerabilities in their equipment. The faulting companies will be held responsible and subject to penalties, if they do not address the vulnerabilites even after communication.
- The government has notified **National Critical Information Infrastructure Protection Centre (NCIIPC),** under the auspices of National Technical Research Organisation, as the nodal agency with respect to Critical Information Infrastructure Protection. The NCIIPC aims to reduce the vulnerabilities of CII against cyber terrorism, cyber warfare and other threats. It is tasked with:
  - Identification of all CII elements;
  - Providing strategic leadership and coherence across government; and
  - Coordinating, sharing, monitoring, collecting, analysing and forecasting national level threat to CII for policy guidance, expertise sharing and situational awareness.
  - Exchange of knowledge and experiences with CERT-IN and other organisations is done for better coordination.

Measures taken to address the misuse of technology by extremists

UNSC's Delhi Declaration on countering the use of new and emerging technologies for terrorist purposes

Financial Action Task Force issued guidelines in 2018 to **regulate virtual assets**

Use of **Facial Recognition Technology by Indian Army** in counter-terrorism operations

Global Counterterrorism Forum has adopted **Berlin Memorandum on Good Practices to Counter Terrorist use of Unmanned Aerial Systems**

8. Way Forward

Communication networks form the core of critical infrastructure of our country. Any disruption to communication networks would have huge implication on stability of India and so their protection is essential to maintenance of internal security of India. Due to its importance, now communication network itself is considered as critical infrastructure. Few points to keep in mind while forging a strategy to secure communication network-

- Today, significant part of critical infrastructure and CII is developed, operated and maintained by the private sector. The private firms typically know more about their system architecture and are in a better position to know about weaknesses that intruders might exploit. On the other hand, the government's highly skilled intelligence agencies typically know more than the private sector about malware used by foreign governments and how to defeat it. This suggests that responsibility for defending the most sensitive systems against the most sophisticated adversaries should be shared.
- The government should take measures for domestic production of critical equipment of communications network through Make in India. For example, rolling out of 5G infrastructure should focus on indigenisation.
- Therefore, government have to move beyond their traditional roles as regulators, and rather forge partnerships with private sector.
- It is essential for both the private and public sectors to **foster the trust and confidence** which is vital to information sharing and success of any policy measure adopted to protect the critical infrastructure.
- Going forward, the protection strategy for critical infrastructure and CII has to **address technological, policy and legal dimensions.**
- From global perspective, India is a key stakeholder in the future of cyberspace governance. As a progressive economy relying upon its CII, It has to pitch its voice to preserve its national interests at various multilateral forums.
- Increase in investments in R&D in securing communications network through developing state of the art security infrastructure and staying a step ahead of attack technology.
- Use of Artificial Intelligence and Machine learning for better prediction and identification of digital security attacks and breaches.

9. UPSC Mains Previous Years' Questions

1. **Use of internet and social media by non-state actors for subversive activities is a major security concern. How have these been misused in the recent past? Suggest effective guidelines to curb the above threat. (2016)**
2. **Discuss the advantage and security implications of cloud hosting of server vis-a-vis in-house machine-based hosting for government businesses. (2015)**

10. Previous Years Vision IAS GS Mains Test Series Questions

1. What is invisible warfare? Keeping in view the challenges it poses to India's security, discuss the steps that have been taken to tackle the menace of invisible warfare.

Approach:

- Define invisible warfare in the introduction.
- Discuss various challenges it poses to India's internal security.
- Highlight the steps that have been taken to tackle these challenges.
- Conclude accordingly.

Answer:

Invisible warfare can be understood as a battle of misinformation and perception. It is conducted through non-kinetic military actions, which have minimal involvement of brute force. They are fought with soft forces of diplomacy, social engineering, cyber-attacks and sanctions. Due to incorporation and usage of technology in its conduct, invisible warfare is also referred to as **'fifth generation warfare'** or 'non-kinetic warfare'.

Following are the challenges invisible warfare poses to India's internal security:

- **Threat to critical sectors:** Infrastructures like banking and telecom have become vulnerable to malware attacks, crypto jacking, phishing attacks etc. It can compromise the strategic information of the nation. **E.g., Cosmos bank cyber-attack, UIDAI information hijack, AIIMS ransomware attack etc.**
- **Data tracking and information hijacking:** The import of foreign made software and service provisioning have increased exponentially. These are often laced with inbuilt malware, which can easily sabotage the system and may lead to information transfer. **E.g., Gionee case of malware implantation.**
- **Misinformation and fake news:** Propaganda and misinformation can be used to sow seeds of discontentment and suspicion in the mind of citizenry against the government, which can adversely impact the overall peace and security of the nation.
- **Damaging country's social fabric:** Intentional circulation and release of communally charged videos create religious animosity that can disturb the communal harmony.
- **Promoting secessionist tendencies:** India has long faced the brunt of provoking narratives by neighbouring countries. These are to incite disenchantment among border states through coveted and diplomatic narrative building. States of erstwhile J&K, Punjab and Arunachal Pradesh have seen instances which threaten the unity of the country.
- **Global espionage and spying:** Penetration of digital technology has made India highly vulnerable to global espionage and spying attempts. International forces have already spread their web of technological espionage across the country. **E.g., espionage on Bharat Biotech, SII (during COVID vaccine development) by Chinese hacker Stone Panda.**

Steps taken to tackle challenges of invisible warfare:

- **National Cyber Security Strategy:** It proposes a three-pronged approach- people, processes and technology.

- For people, it mandates increasing cyber hygiene, and the number of cybersecurity professionals.
- For processes, it proposes SOPs, a management plan for a cyber crisis and privileges to ensure that minimum access is given to users.
- The technology vertical would address the need for firewalls, installation of intrusion prevention systems, behavioural analysis tools, network segmentation and creation of offline backups.

- **The Indian Computer Emergency Response Team (CERT-In):** It is the national bureau for event response, including evaluation, prediction and alerts for cybersecurity breaches. It offers technical support and guidance on how to recover from computer security incidents.
- **The Cyber Swachhta Kendra:** It aims to create a secure cyberspace by identifying botnet infections in India and alerting, facilitating the cleaning process along with securing systems of end users to avoid future infections.
- **NATGRID:** It is an integrated intelligence master database structure that links databases from several security agencies within the Government of India. It collects detailed patterns obtained from numerous organizations and makes them easily accessible to security agencies around the clock.
- **Stringent regulations and strategies:** Ministry of Home Affairs has approved creation of the National Counter Ransomware Task Force.

India has one of the highest numbers of internet users. With the ever-changing cyber security landscape, a good security plan is needed which must include regular technology upgrades, awareness, skilling and reskilling of all stakeholders.

2. With adequate examples, explain how fake news can be a threat to national security. What measures can be taken to counter this threat?

Approach:

- Briefly explain the meaning of fake news.
- Discuss the potential of fake news in affecting national security.
- List the measures to counter threat of fake news.
- Conclude appropriately.

Answer:

Fake news refers to **false or misleading information presented as authentic news** to misinform and deceive readers. The objective is to **influence the readers' views, push a political agenda or cause confusion amongst the public.** Fake news can be in the form of state sponsored misinformation campaigns, commercially driven sensational content, biased news, misleading headings and satire or parody.

With **technological development and increased access to the internet,** the spread of fake news has gained momentum in recent times. It has the potential to become a **threat to national security** in following manner:

- **Disturbing law and order:** Fake news in the wake of violence, disaster or terrorist attack creates social turmoil, put public life to a halt and creates a law and order situation. For instance, **in March 2020 false rumours of violence sparked panic among people in various parts of Delhi** and even led to temporary shutdown of few metro stations.

- **Promotes mob culture in society:** Using fake news for creating hatred, polarizing public opinion, inciting extremism and hate speech ultimately undermines people's trust in the public institutions and processes. For example- viral **false messages about child kidnappers on WhatsApp** has led to **killing of two dozen innocent people** by fearful mobs.
- **Aggravating existing social divisions/tensions:** Spreading misinformation to inflame the existing social conflicts in the society like ethnic or communal can create tension and violence. For instance a **fake video shared on WhatsApp resulted in communal riots in 2013** leading to the death of 62 people and displacement of 50,000 people **in Western Uttar Pradesh.**
- **State sponsored disinformation campaign:** Run by the **nations against their rivals with the aims of destabilizing** them through subversion of societies and democratic processes including elections. For example- the Russian authorities have been accused of interfering with state elections in Europe and America.

According to a Microsoft study, 64 percent of Indians encountered fake news online. These figures pose huge challenge for the authorities and necessities the implementation of effective measures to counter the threats paused by fake news:

- **Create adequate legal framework:** Apart from, limited period internet shutdowns or blocking or deleting the accounts of culprits, the government should enact law to prevent circulation of fake news affecting national security as done by **Singapore** which passed **Protection from Online Falsehood and Manipulation Act (POFMA) in 2019.**
- **Fixing accountability of intermediaries:** Enforcing legal provisions to f**ix responsibilities of search engines and social messaging platforms** such as WhatsApp, Twitter, YouTube and Facebook. Further, social media houses should undertake voluntary measures to curb the menace of fake news.
- **Initiate education and awareness campaign: Educating people especially children about the misuse of social media** and enabling them to identify fake news and prevent its recycling.
- **International partnerships:** India should **partner with like-minded countries** like Singapore to counter fake news on an international level. The signing of **the "Christchurch Call to Action"** declaration by India is a step in the right direction.

The government should also make use of existing provisions of the IT (Amendment) Act 2008 in respect of monitoring and blocking websites which spread misinformation. The **Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021,** which have been framed in exercise of powers under section 87 (2) of the Information Technology Act, 2000 and in supersession of the earlier Information Technology (Intermediary Guidelines) Rules 2011, are a step in this direction.

3. What are the threats posed by communication networks to internal security of India?

Approach:

Students should begin by giving the importance and relevance of communication networks to the country in a paragraph. Thereafter the answer should focus on loopholes in the communication networks that pose a threat to national security.

Answer:

Communications networks are crucial to the connectivity of other critical infrastructure, viz. civil aviation, shipping, railways, power, nuclear, oil and gas, finance, banking, communication, information technology, law enforcement, intelligence agencies, space, defence, and government networks. Therefore, threats can be both through the networks as well as to the networks.

- Securing the networks is complicated by a number of factors. For example, much of the hardware and software that make up the communications ecosystem is sourced externally; as a case in point, Chinese manufacturers such as Huawei and ZTE have supplied about 20 per cent of telecommunications equipment while Indian manufacturers have about 3 per cent of the market
- As recent incidents have shown, foreign governments are not behind in taking advantage of the market penetration and dominance of their companies to infiltrate and compromise telecommunications networks.
- Expanding wireless connectivity to individual computers and networks has increased their exposure and vulnerability to attacks. The traditional approach of securing the boundaries are not effective in this space.
- Evolution of communication networks has made communication system more user-friendly and accessible. This had made it possible for miscreants in the society to use these tools for their benefits.
- It has become really difficult to track a message through VOIP services & various other services. This has served to spread terrorism ideology even across liberal population sphere.
- In the not-too-distant future, major powers will be focused on the proliferation of weapons of mass destruction, terrorism, narcotics, and organized crime more than conventional armed conflicts. Information warfare, threats emanating from cyber space and aerospace will consume more national resources than ever before.
- Few other ways which are impacting the security of the country are, knowledge of strategic location, important spots, private identity of people & use of that in malware documents, cyber attack on strategic infrastructure etc.

4. ICT revolution is not only a great equalizer for smaller states, but has also brought power to non-state actors, individuals and terrorist organizations. Examine the statement in the context of challenges to India's national security.

Approach:

Firstly, elaborate on the first statement, quoting various examples. Then bring out the challenges associated in the realm of cyberspace which could be a threat to India's National security and suggest measures for tackling the same.

Answer:

The ICT revolution has brought new challenges to state's internal security apparatus. The dependence of not only state's critical infrastructure on ICT but of the whole system encompassing military, administrative and economic apparatus has increased vulnerability of the system not only among states but also to non-state actors which could destabilize the whole system with the speed of a light.

The effect of ICT on warfare is evident in command and control, in the new surveillance and communication technologies and in cyber operations.

Between states, information technologies and their effects have made asymmetric strategies much more effective and attractive. In situations of conventional imbalance between states we see that asymmetric strategies are increasingly common. **Cyber war and anti-satellite capabilities are uses of technology by a weaker state to neutralise or raise the cost and deter the use of its military strength by a stronger country.** Currently, In the name of defence all the major powers are developing offensive cyber capabilities as well as using cyber espionage and so are smaller powers that see ICT as an equaliser.

These technologies have also enabled individuals and small groups to use cyberspace for their own ends **The ICT revolution has also brought power to non-state actors and individuals, to small groups such as terrorists.** ICT helps Terror organisation in Propaganda, Financing, Training, Planning and Execution of their agendas.

Thus it has given small groups and individuals the means to threaten and act against much larger, more complex and powerful groups. Since the technology is now available or accessible widely, and is mostly held in private hands, ICT has redistributed power within states.

Challenges to internal security of India

The technology has placed an increasingly lethal power in the hands of non-state actors. These are not just law and order problems, and they are not amenable to the traditional responses that states are accustomed to.

What makes this more complicated is the fact that these technologies are not just available to the state, where laws and policies can control and limit their use. **They are widely available in the public domain, where commercial and individual motives can easily lead to misuse that is not so easily regulated unless we rethink and update our legal and other approaches.**

Expanding wireless connectivity to individual computers and networks has increased their exposure and vulnerability to attacks. The traditional approach of securing the boundaries are not effective in this space.

Evolution of communication networks has made communication system more user-friendly and accessible. This had made it possible for miscreants in the society to use these tools for their benefits.

It has become really difficult to track a message through VOIP services & various other services. This has served to spread terrorism ideology even across liberal population sphere.

Thus need is to create a climate and environment within which security is built into the cyber and communications working methods. And, most important, the government must find ways to indigenously generate the manpower, technologies and equipment that it requires for maintaining cyber security.

5. Threats to internal security of India may be posed both through the communication networks and also to the networks. Discuss. Also, highlight the steps taken by the government in making the networks more secure.

Approach:

- Briefly explain the interdependence between communication network and internal security of India.
- Explain the threats posed to and from such networks.
- Explain some critical challenges associated with resolving these threats.
- Highlight the steps taken by government in this regard.

Answer:

IT Act 2000 considers communication network as a part of critical information infrastructure whose incapacitation or destruction can have debilitating impact on national security, economy, public health or safety.

The following factors make vulnerability of communications networks serious:

- Interconnectedness of sectors
- Proliferation of exposure points
- Concentration of assets

Therefore, threat to the internal security emanates both through the communication network and to it.

Threats from/through the network:

- It includes hacking, data theft, cyber-frauds, cyber terrorism with the help of viruses, worms, botnets, phishing, etc. This can have adverse effect over government systems, business ecosystems and financial institutions such as banks and stock exchange.
- These networks can be used by terrorist groups for communication, transfer of funds, radicalization and spreading extremist ideologies.

Threats to the network:

- Nation states, non-state actors and individuals can negatively impact data integrity, information privacy and network availability of communication networks.
- Attacks on communication networks endanger the connectivity of other critical infrastructures such as civil aviation, shipping, railways, power, nuclear, oil and gas, finance, banking, communication, information technology, law enforcement, intelligence agencies, space, defence, and government networks.

However, securing the communication network in India remains a complex task because a significant part of hardware and software that make up the communications ecosystem is sourced externally, which increases its vulnerability.

In view of this, the Government of India has taken following steps:

- **Developing security standards** such as Telecom Testing and Security Certification for equipment and devices; **aligning them with global standards & harmonizing** the existing legal & regulatory framework.
- **Strengthening security testing processes** by both establishing comprehensive security **certification regime** & enhancing **institutional capacity** through domestic testing hubs and laboratories with state-of-the art facilities.
- Formulating a **policy on encryption and data retention,** by harmonising the legal and regulatory regime in India pertaining to cryptography with global standards, as applicable to communication networks and services.
- Facilitating security and safety of citizens by establishing **Central Equipment Identity Registry** for addressing security, theft and other concerns.
- Facilitating **lawful interception of all digital communications** with state of the art lawful intercept and analysis systems for implementation of law and order and national security
- Increasing **awareness** amongst users about security related issues concerning digital communications networks, devices and services.
- Establishing a Security Incident Management and Response System through **sectoral Cyber Security Incidence Response System (CSIRT).**
- Improving **information sharing and coordination between various security agencies,** including CERT-In and sectoral CERTs as may be necessary.

Heartiest Congratulations to all Successful Candidates

Aditya Srivastava

16 in **TOP 20** Selections in **CSE 2023** from various programs of **Vision IAS**

Animesh Pradhan

Ruhani

Srishti Dabas

Anmol

Nausheen

Aishwaryam Prajapati

39 Selections in **TOP 50** in **CSE 2022**

Ishita Kishore

Garima Lohia

Uma Harathi N

SHUBHAM KUMAR

CIVIL SERVICES EXAMINATION 2020

HEAD OFFICE
Apsara Arcade, 1/8-B 1st Floor, Near Gate-6 Karol Bagh Metro Station
DELHI

MUKHERJEE NAGAR CENTER
Plot No. 857, Ground Floor, Mukherjee Nagar, Opposite Punjab & Sindh Bank, Mukherjee Nagar

GTB NAGAR CENTER
Classroom & Enquiry Office, above Gate No. 2, GTB Nagar Metro Building, Delhi - 110009

FOR DETAILED ENQUIRY
Please Call:
+91 8468022022,
+91 9019066066

enquiry@visionias.in /c/VisionIASdelhi /visionias.upsc /vision _ias VisionIAS_UPSC

AHMEDABAD BENGALURU BHOPAL CHANDIGARH DELHI GUWAHATI HYDERABAD JAIPUR JODHPUR LUCKNOW PRAYAGRAJ PUNE RANCHI

VISIONIAS
INSPIRING INNOVATION

Classroom Study Material

INTERNAL SECURITY

MONEY LAUNDERING & its Prevention

AHMEDABAD BENGALURU BHOPAL CHANDIGARH DELHI GUWAHATI HYDERABAD JAIPUR JODHPUR LUCKNOW PRAYAGRAJ PUNE RANCHI

Contents

1. Introduction

Prevention of Money-Laundering Act, 2002 defines the offence of 'Money Laundering' as, "Whosoever directly or indirectly attempts to indulge or knowingly assists or knowingly is a party or is actually involved in **any process or activity connected with the proceeds of crime and projecting it as untainted property shall be guilty of offence of money-laundering**".

In simple terms, Money laundering is the process of taking money earned from illicit activities, such as drug trafficking or tax evasion, and making the money appeared to be earnings from legal business activity.

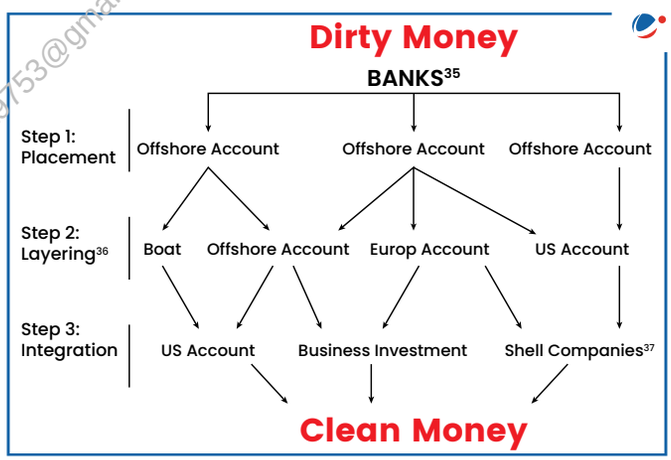
1.1. Why is Money Laundered?

Illegal arms sales, smuggling, and other organized crime, including drug trafficking and prostitution rings, can generate huge amounts of money. Corruption, embezzlement, insider trading, bribery and computer fraud schemes can also produce large profits. The money generated from such illicit activities is considered **dirty** and needs to be laundered to make it look '**clean**'. The criminals need a way to deposit the money in financial institutions. Yet they can do so if the money appears to come from legitimate sources. By successfully laundering the proceeds, the proceeds can be made to appear 'clean' and the illicit gains may be enjoyed without fear of being confiscated or being penalized.

1.2. How is Money Laundered?

Traditionally money laundering has been described as a process which takes place in three distinct stages.

Placement Stage – At this stage criminally derived funds are introduced in the financial system. This is the **riskiest stage** because of large amounts of cash involved which can catch the eyes of law enforcement agencies. So the launderer breaks large amounts of cash into less conspicuous smaller sums that are then deposited directly into a bank account, or is used to purchase monetary instruments such as cheques, money orders etc.



Layering stage - It is the stage at which complex financial transactions are carried out in order to camouflage the illegal source. In other words, the money is sent through various financial transactions so as to change its form and make it difficult to follow. Layering may be done by below mentioned ways.

- Several bank-to-bank transfers which may be in small amounts.
- Wire transfers between different accounts in different names in different countries.
- Making deposits and withdrawals to continually vary the amount of money in the accounts.
- Changing the money's currency.
- Purchasing high-value items such as houses, boats, diamonds and cars to change the form of the money.
- Disguising the transfers as payments for goods or services provided.

Integration stage – This is the final stage at which the 'laundered' property is **re-introduced into the financial system as legitimate money**. At this stage, the launderer might choose to invest the funds into real estate, luxury assets, or business ventures. At this point, the launderer can use the money without getting caught. It's very difficult to catch a launderer during the integration stage if there is no documentation during the previous stages.

1.3. Various Techniques Used for Money Laundering

EVOLUTION OF MONEY LAUNDERING TECHNIQUES

Hawala: (India)

- In hawala, funds are moved between individual "hawaladars which collect funds at one end of the operation and other hawaladars that distribute the funds at the other end

Cyber Crime

- Cyber crimes such as identity theft, illegal access to e-mail, and credit card fraud are coming together with money laundering and terrorist activities

Third Party Cheques

- Utilizing counter cheques or banker's drafts drawn on different Institutions and clearing them via various third-party accounts
- Since these are negotiable in many countries, the nexus with the source money is difficult to establish

Open Securities Market

- Laundering is possible due to the instruments like hedge funds and participatory notes which have very limited disclosures as to the source

Casinos: (North America)

- The cash intensive nature of the casino business and the size of transaction frequency and volumes had made it vulnerable to money laundering
- North America accounted for around 50% of the global casino market even as late as 2009

Insurance Sector

- If a money launderer is able to move funds into an insurance product and receive a payment made by an insurance company then he or she will have made the funds appear legitimate

Structuring

- Depositing of cash or purchasing of bank drafts at various institutions by several individuals, or carrying out of transactions below reporting thresholds

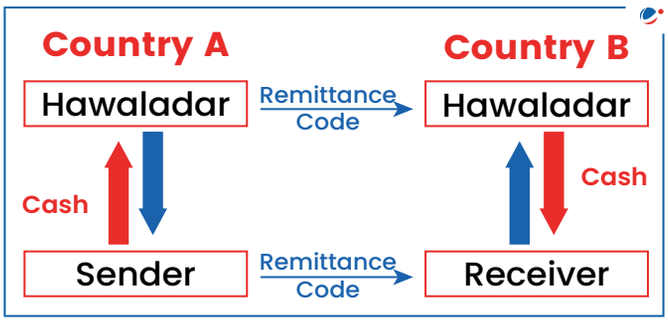
Credit Cards

- Creating credit on a card by paying cash on the card allowing the credit to be converted to cash

- **Structuring Deposits**: This is a method of placement whereby cash is broken into smaller deposits of money which is then exchanged by many individuals (known as "smurfs") to avoid anti-money laundering reporting requirements. This is also known as smurfing because many individuals (the "smurfs") are involved.
- **Shell companies**: These are companies without active business operations. They take in dirty money as "payment" for supposed goods or services but actually provide no goods or services; they simply create the appearance of legitimate transactions through fake invoices and balance sheets.
- **Third-Party Cheques**: Counter cheques or banker's drafts drawn on different institutions are utilized and cleared via various third-party accounts. Since these are negotiable in many countries, the nexus with the source money is difficult to establish.
- **Bulk cash smuggling**: This involves physically smuggling cash to another jurisdiction and depositing it in a financial institution, such as an offshore bank, with greater bank secrecy or less rigorous money laundering enforcement.
- **Credit Cards**: Clearing credit and charge card balances at the counters of different banks. Such cards have a number of uses and can be used across international borders. For example, to purchase assets, for payment of services or goods received or in a global network of cash-dispensing machines

1.4. Hawala and Money Laundering

The word "Hawala" means trust. Hawala is a system of transferring money and property in a parallel arrangement avoiding the traditional banking system. It is a simple way of money laundering and is banned in India.



How it works?

In a hawala transaction, **no physical movement of cash** is there. Hawala system works with a network of operators called Hawaldars or Hawala Dealers. A person willing to transfer money, contacts a Hawala operator ('**A**' in the figure) at the source location who takes money from that person. The **Hawala operator** then calls upon his counterpart ('B') at the destination location who gives the cash to the person to whom the transfer has to be made, thus completing the transaction.

Status of Hawala in India

- Hawala is illegal in India, as it is seen to be a form of money laundering.
- As hawala transactions are not routed through banks, the 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 legislation which make such transactions illegal.

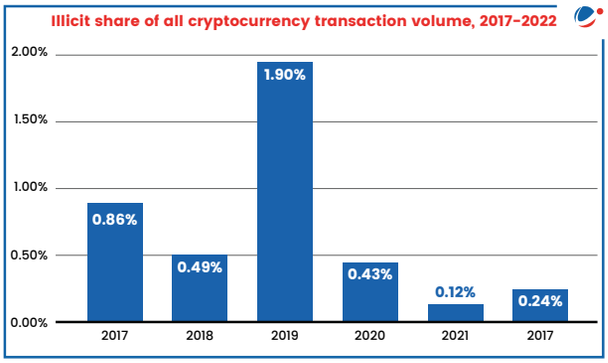
Hawala network is being used extensively across the globe to circulate black money and to provide funds for terrorism, drug trafficking and other illegal activities. Despite the fact that hawala transactions are illegal, **people use this method because of the following reasons**:

- The commission rates for transferring money through hawala are quite low.
- No requirement of any id proof and disclosure of source of income.
- It has emerged as a reliable and efficient system of remittance.
- As there is no physical movement of cash, hawala operators provide better exchange rates as compared to the official exchange rates.
- It is a simple and hassle free process when compared to the extensive documentation being done by the banks.
- It is the only way to transfer unaccounted income.

1.5. Cryptocurrency and Money Laundering

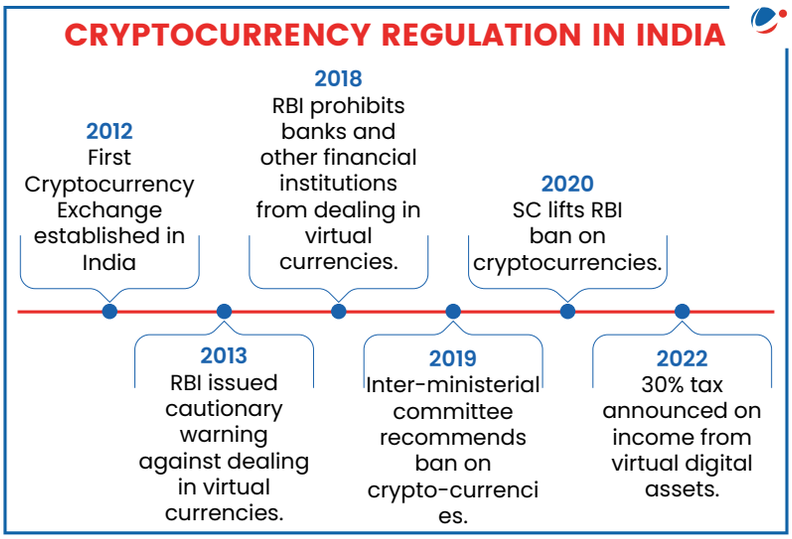
A cryptocurrency is a **digital or virtual currency** that uses cryptography for security. A defining feature of a cryptocurrency is its **fundamental nature**: it is not issued by any central authority, rendering it theoretically immune to government interference or manipulation.

In 2021, illicit transactions using cryptocurrencies were estimated to be $14 billion, 79% increase from $7.8 billion the previous year.



Cryptocurrencies pose a significant challenge for financial institutions and anti-money laundering programs. While investors are currently active in this market, formal regulations are still evolving in many countries.

Currently, there are no national guidelines on cryptocurrency related cases, due to which enforcement agencies often struggle, particularly in seizure as well as tracing suspects.

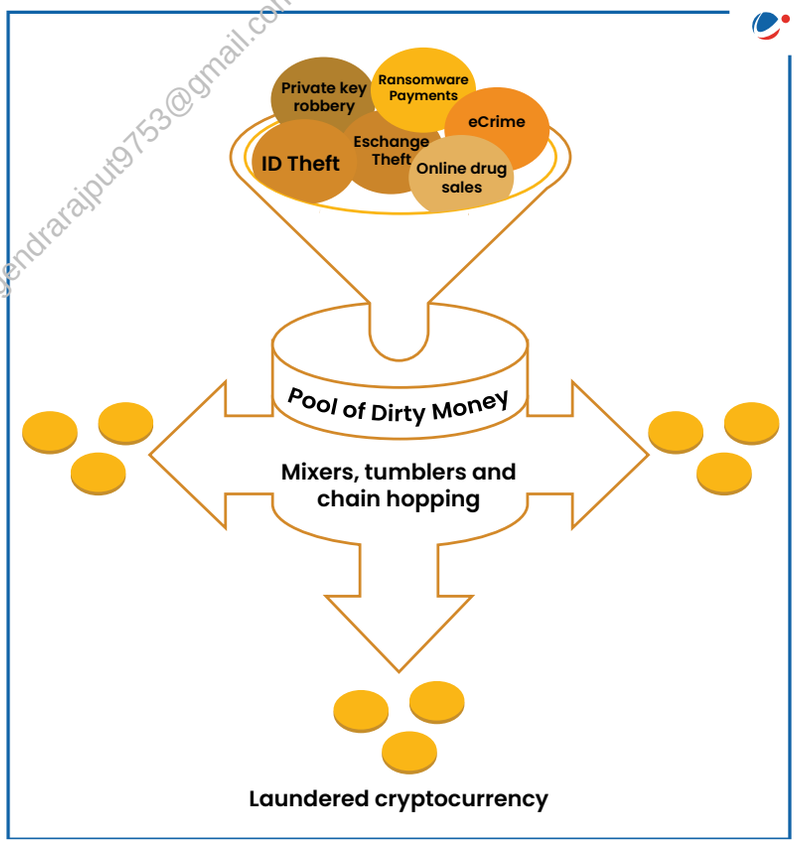


ML Services for CC

There are a number of money laundering services available for cryptocurrencies. These services are variously called mixers, tumblers, foggers and laundries. They take in funds from multiple customers, mix those funds together, and then output the **mixed funds**. The purpose of these money laundering services is to obfuscate the origin and receipt of cryptocurrencies. Some of the well-known cryptocurrency ML services include Bitcloak, Darklaunder, Bitmixer, Bitblender, etc.

How does Cryptocurrency Money Laundering Work?

The growing theft of cryptocurrencies and their increasing use by terrorists, extortionists, identity thieves, drug dealers, weapons dealers and human traffickers has ushered in a new era of high-tech virtual money laundering. However, unlike cash, getting this dirty crypto money clean is a little more complicated. The steps included in the process are:



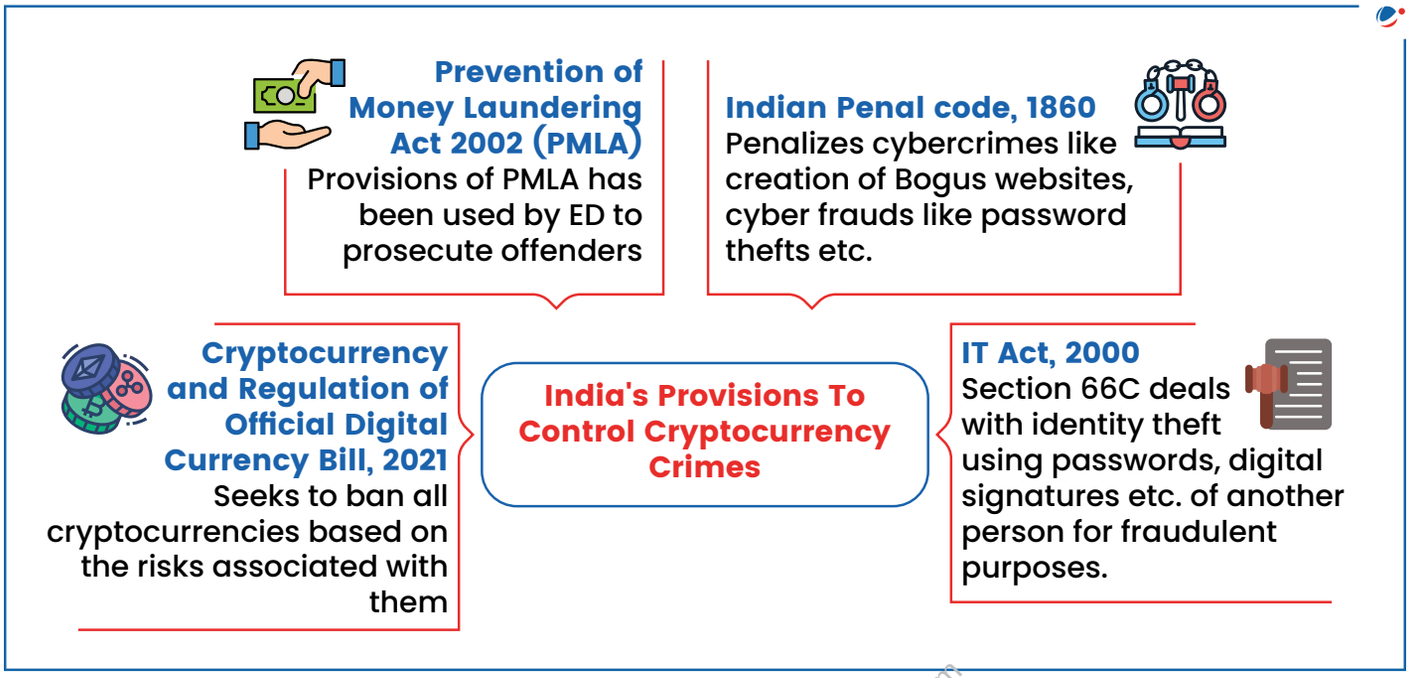
Layering

- In the traditional money laundering world, this would involve purchasing expensive items like gold bars, cars, jewelry or real estate, and then reselling them. In the virtual world, it involves moving money into the cryptocurrency system and moving it around by using **mixers, tumblers and chain hopping**. The more dirty crypto money that goes into the systems and the more it moves around, the harder it becomes for investigators to see through the web of action and trace a path back to the source.
- The **pseudo-anonymous nature** of virtual currencies makes it exponentially more difficult to trace these funds as compared to cash. As one caveat, criminals will lose a percentage off the top to move the funds, but in the end the funds appear legitimate, making the loss worthwhile.

Integration

- After placing the funds in the cryptocurrency system and moving them around in a kind of virtual shell game, the criminals are closer to enjoying unencumbered and relatively safe use of their ill-gotten gains.

- There are still risks to integrating the funds into the mainstream financial system because exchanges and other parties involved in cryptocurrency transactions monitor activity and may issue **Suspicious Activity Reports (SARs)**, which flag high-risk transactions. However, once legitimized, the criminals have multiple options for recouping the funds from the financial system.



1.6. Illegal Wildlife Trade (IWT) and Money laundering

The Financial Action Task Force (FATF) released it's **first-ever report on illegal wildlife trade (IWT).** The report comes amid increasing international concern that the crime could lead to more zoonotic diseases in the future.

Findings of the report

- The illegal wildlife trade (IWT) is a major **transnational organised crime** that fuels corruption, threats biodiversity, and can have significant public health impacts. In particular, the spread in recent years of **zoonotic diseases** underlines the importance of ensuring that wildlife is traded in a legal, safe and sustainable manner, and that countries remove the profitability of illegal market.
- India has also been a source country for **illegal pangolin trading**. Talking about the extravagant mark-ups of illegal wildlife trade, the report points out that the price of **rhinoceros' horn** can reach about $65,000 per kg, but has also been known to be as low as $9,000 per kg.
- **Syndicates** involved in wildlife crime usually poach, harvest or breed wildlife in countries that are rich in biodiversity and/or where there may be weaker law enforcement oversight and criminal justice — or in source countries.
- To hide the real **country of origin**, criminals involved in IWT often divert containers or shipments through third countries, and switch the bills of lading or vessel. For the sale of the illegal wildlife, jurisdictions identified common use of cash, mobile or social media-based payments, and third party payments.
- Countries reported that criminals involved in IWT are **placing and layering funds** through cash deposits (under the guise of loans or payments), e-banking platforms (e.g., electronic payment services that are tied to a credit card or bank account) and licensed money value transfer systems (MVTS) like **'hawala', 'hundi' and 'fei chen'** which are usually community-based and draw on a network of brokers across countries to facilitate international transfers without money physically crossing borders. Third-party wire transfers through banks are also used.

- **Legitimate pet stores** and private "zoos", "farms" or "parks" are often used to facilitate the illicit pet trade in many countries (such as Asia and the Americas) and are used to justify trading, breeding, or otherwise exploit protected wildlife. The financial flows associated with this type of IWT activity are often significant, stated the report, mentioning that "tiger zoos" with a large number of tigers have profited from selling tiger cubs and parts.
- **New technologies** play an important role in facilitating communication and non-face-to-face payments between buyers and sellers for illegal wildlife.
- In particular, encrypted communication platforms and illegal wildlife marketplaces hosted via social media sites, online vendor platforms, and the dark net increase the ease with which wildlife transactions can occur between buyers and sellers.

2. Impact of Money Laundering on Nation

Money laundering is a problem not only in the world's major financial markets and offshore centers, but also for emerging markets. It has potentially devastating economic, security, and social consequences for the nation.

- **Social Impact:** It damages social institutions by following ways:
  - The social impact of strong illegal businesses includes increased drug addiction, rampant corruption, and criminals empowered with economic powers.
  - Transfers the economic power from the right people to the wrong ones.
  - Loss of morality and ethical standards leading to weakening of social institutions.
  - Increased unemployment as legitimate business companies fail to compete with operators operating through illegal money.
- **Economic Impact:**

Microeconomic impacts of money laundering are as following:

- Potential damage to reputation of financial institutions and market.
- Policy distortion occurs because of measurement error.
- Legitimate businesses lose when competing, as there is no fair competition involved.
- Organised crime at the local level may flourish.
- It also leads to a higher cost of doing business, which adversely affects small businesses disproportionately.

Macroeconomic impacts of money laundering are as following:

- These include volatility in exchange rates and interest rates due to unanticipated transfers of funds.
- Fall in asset price due to the disposition of laundered funds.
- Misallocation of resources in relative asset commodity prices arising from money laundering activities.
- Loss of confidence in markets caused by insider trading, fraud and embezzlement.
- Discourages foreign investors as high level of corruption is seen as unfavorable for businesses.
- Other indirect economic effects are higher insurance premiums for those who do not make fraudulent claims and higher costs to businesses therefore generating fewer profits which make it difficult to break even.
- Due to such negative impact, policy makers have to face difficulty to devise effective responses to monetary threats and it causes difficulties in the government efforts to manage economic strategy.

All the above points would lead to artificial inflation, jobless growth, income inequality, poverty etc. which culminates in the end to pose security challenges to the society.

- **Political Impact**
  - Affects the government's capability to spend on development schemes thereby affecting a large section of populations who could have benefitted from such spending.

- Legislative bodies find it difficult to **quantify the negative economic effects** of money laundering on economic development and its linkages with other crimes – trafficking, terrorism etc.

Security Impact

- The quest to legalize illicit earnings spawns money laundering, which in turn provides the required financial boost for these illegal activities to survive. Several large-scale illegal activities such as arms dealing, organized crime, terrorist financing, as well as drug and sex trafficking, do not just drive money laundering but thrive on it.
- Usually terrorist organisations receive funds from other countries, those funds cannot be transferred easily through formal banks, so terrorists use hawala transaction for receiving and sending all the funds.

3. Prevention of Money Laundering

Anti-money laundering involves the laws and regulations designed to prevent criminals from generating income through illegal activities. The government has become increasingly vigilant in its effort to curb money laundering by passing anti-money laundering regulations. These regulations require financial institutions to have systems in place to detect and report suspected money laundering activities.

2023 Amendment to the Prevention of Money Laundering (Maintenance of Records) Rules, 2005

- **Tightened the definition of beneficial ownership:** Any individual or group holding 10% ownership in the client of a "reporting entity" will now be considered a beneficial owner as against the ownership threshold of 25% applicable earlier.
  - Under the anti-money laundering law, "reporting entities" are banks and financial institutions, firms engaged in real estate and jewelry sectors.
  - They also include intermediaries in casinos and crypto or Virtual digital assets (VDAs).
- **Expanded the due diligence requirement:** Rules prescribes disclosures of beneficial owners beyond current requirement of KYC norms through documents such as registration certificates and PAN.
  - Reporting entities are required to register details of the client if it's a non-profit organisations on the DARPAN portal of NITI Aayog.
- **Politically Exposed Persons (PEPs):** Amendment defines PEPs as individuals who have been entrusted with prominent public functions by a foreign country, including Heads of States/ Governments, senior politicians etc.
- **Widened the definition of Non-profit organisations.** It now includes:
  - any entity or organisation constituted for religious or charitable purposes referred to in Section 2 of the Income-tax Act, 1961.
  - registered as a trust or a society under the Societies Registration Act, 1860 or any similar state legislation.

  a company registered under Section 8 of the Companies Act, 2013

3.1. Indian Mechanisms to Combat Money Laundering

3.1.1. Prevention of Money Laundering Act, 2002 (PMLA)

- It is a comprehensive law enacted by the Parliament of India to prevent money-laundering and to provide for confiscation of property derived from money laundering.
- Under the Act, Enforcement Directorate (ED) is empowered to conduct money laundering investigation.
- The Act and Rules notified thereunder impose obligation on banking companies, financial institutions and intermediaries to verify identity of clients, maintain records and furnish information in prescribed form to Financial Intelligence Unit – India (FIU-IND).
- It seeks to bring certain financial institutions like Full Fledged Money Changers, Money Transfer Service and Master Card within the reporting regime of the Act.
- It adds a number of crimes under various legislation in Part A and Part B of the Schedule to the Act for the purpose of money-laundering.

- In cases of cross-border money-laundering the Act enables the Central Government to return the confiscated property to the requesting country in order to implement the provisions of the UN Convention against Corruption.
- The Act prescribes for formation of a three-member Adjudicating Authority for dealing with matters relating to attachment and confiscation of property under the Act.

Amendments to the PMLA (2019)

The basic aim of the amendment is to empower the ED for tackling the cases of money laundering. The following are the amendments made:

- The definition of "**proceeds of crime**" has been widened which now includes properties and assets created through any criminal activity even if it is not under the Prevention of Money Laundering Act (PMLA) and it will now be considered as "**relatable offence**".
- It seeks to treat the offence of money laundering as a stand-alone crime.
- Deletion of provisions which required the prerequisite of an FIR or chargesheet by other agencies that are authorised to probe the offences listed in the PMLA schedule.
- All PMLA offences will be cognisable and non-bailable. Therefore, the ED will be empowered to arrest the accused without a warrant, subject to certain conditions.
- Another vital amendment makes concealment of proceeds of crime, possession, acquisition, use, projecting as untainted money, or claiming as untainted property as independent and complete offences under the Act.

3.1.2. Financial Intelligence Unit - India (FIU-IND)

- Financial Intelligence Unit – India (**FIU-IND**) was set by the Government of India in 2004 as the central national agency responsible for **receiving, processing, analyzing and disseminating information** relating to suspect financial transactions.
- FIU-IND is also responsible for **coordinating and strengthening efforts** of national and international intelligence, investigation and enforcement agencies in pursuing the global efforts against money laundering and related crimes.
- FIU-IND is an **independent body** reporting directly to the Economic Intelligence Council (EIC) headed by the Finance Minister.

3.1.3. Enforcement Directorate

- The ED, established in 1956, is a multi-disciplinary organisation mandated to enforce two pivotal fiscal laws:
  - **Foreign Exchange Management Act, 1999 (FEMA)**: This civil law with quasi-judicial powers investigates contraventions of exchange control laws and imposes penalties.
  - Prevention of Money Laundering Act, 2002 (PMLA): This is a criminal law that empowers officers to conduct inquiries, attach/confiscate assets, and prosecute money launderers.
  - Other laws and acts that the ED can enforce include:
    - **Fugitive Economic Offenders Act, 2018 (FEOA)**: This act enables action against criminals who fled the country after committing economic crimes.
    - **Conservation of Foreign Exchange and Prevention of Smuggling Activities Act, 1974 (COFEPOSA)**: This act helps prevent smuggling activities.
- The Directorate is under the **administrative control of Department of Revenue** for operational purposes; the policy aspects of the FEMA, its legislation and its amendments are within the purview of the Department of Economic Affairs.

3.2. Global mechanisms to Combat Money Laundering:

Since money laundering is an international phenomenon, transnational co-operation is of critical importance in the fight against this menace. A number of initiatives have been taken to deal with the problem at the international level. The major international agreements addressing money laundering are as:

3.2.1. Vienna convention

It was the first major initiative in the prevention of money laundering held in December 1988. This convention laid down the groundwork for efforts to combat money laundering by obliging the member states to criminalize the laundering of money from drug trafficking. It promotes international cooperation in investigations and makes extradition between member states applicable to money laundering.

3.2.2. The Council of Europe Convention

This convention held in 1990 establishes a common policy on money laundering to facilitate international cooperation as regards investigative assistance, search, seizure and confiscation of the proceeds of all types of criminality, particularly serious crimes such as drug offences, arms dealing, terrorist offences etc. which generate large profits. It sets out a common definition of money laundering and common measures for dealing with it.

3.2.3. Basel Committee's Statement of Principles

In December 1988, the Basel Committee on Banking Regulations and Supervisory Practices issued a statement of principles which aims at encouraging the banking sector to adopt common position in order to ensure that banks are not used to hide or launder funds acquired through criminal activities.

3.2.4. The Financial Action Task Force (FATF)

The FATF is an inter-governmental body established at the G7 summit at Paris in 1989 with the objective to set standards and promote effective implementation of legal, regulatory and operational measures to combat money laundering and terrorist financing and other related threats to the integrity of the international financial system. It has developed a series of recommendations that are recognized as the international standards for combating money laundering and the financing of terrorism. They form a basis for a coordinated response to these threats to the integrity of the financial system and help ensure a level playing field.

- FATF is the global inter-governmental money laundering (ML) and terrorist financing (TF) watchdog.
  - It sets international standards(recommendations) that aim to prevent these illegal activities.
- Currently comprises 37 member jurisdictions and 2 regional organisations (Gulf Co-operation Council and European Commission).
  - India became a member of the FATF in 2010.
  - FATF suspended Russia's membership over Ukraine war.
- FATF's 'Black' and 'Grey' lists- These terms do not exist in official FATF terminology but are colloquial phrases used to describe two lists of countries maintained by the body.
  - Black List countries- High risk and subject to Call for Action (Myanmar, North Korea, Iran)
  - Grey List Countries- Countries under increased monitoring. FATF recently removed Pakistan from the Grey List.

3.2.5. United Nations Global Programme against Money Laundering (GPML)

GPML was established in 1997 with a view to increase effectiveness of international action against money laundering through comprehensive technical cooperation services offered to Governments. The programme encompasses following **3 areas of** activities, providing various means to states and institutions in their efforts to effectively combat money laundering.

Three further Conventions have been adopted for Money Laundering related crimes:

- International Convention for the **Suppression of the Financing of Terrorism** (1999).
- UN Convention against **Transnational Organized Crime** (2000).
- UN Convention against **Corruption** (2003).

3.2.6. Other Organization and Initiatives towards Anti-Money-Laundering (AML)

- **International Money Laundering Information Network (IMoLIN)**
  - IMoLIN is an Internet-based network assisting governments, organizations and individuals in the fight against money laundering and administered by UN office on Drugs and Crime.
  - It provides with an international database called **Anti-Money Laundering International Database** (AMLID) that analyses jurisdictions national anti-money laundering legislation.
- **Wolfsberg AML Principles**
  - This gives eleven principles as an important step in the fight against money laundering, corruption and other related serious crimes.
  - **Transparency International (TI)**, a Berlin based NGO in collaboration with 11 International Private Banks under the expert participation of Stanley Morris and Prof. Mark Pieth came out with these principles as important global guidance for sound business conduct in international private banking.
  - The importance of these principles is due to the fact that it comes from initiative by **private sector**.
  - The Wolfsberg Principles are a **non-binding set of best practice guidelines** governing the establishment and maintenance of relationships between private bankers and clients.
- **Egmont Group of Financial Intelligence Units**
  - The Egmont Group is the **coordinating body** for the international group of Financial Intelligence Units (FIUs) formed in 1995 to promote and enhance international cooperation in anti-money laundering and counter-terrorist financing.
  - The Egmont Group consists of **165 financial intelligence units (FIUs)** from across the world. Financial intelligence units are responsible for following the money trail, to counter money laundering and terror financing.
  - FIUs participating in the Egmont Group affirm their commitment to encourage the development of FIUs and co-operation among and between them in the interest of combating money laundering and in assisting with the global fight against terror financing.
- **Asia-Pacific Group on Money Laundering (APG)**
  - The Asia/Pacific Group on Money Laundering (APG) is an international organisation consisting of **41 member countries/jurisdictions** and a number of international and regional **observers** including the United Nations, IMF and World Bank.
  - All APG members commit to effectively implement the FATF's international standards for anti-money laundering and combating financing of terrorism referred to as the **40+9 Recommendations**. Part of this commitment includes implementing measures against terrorists listed by the United Nations in the "**1267 Consolidated List**".

4. Challenges in Prevention of Money Laundering

Various measures taken by India against money laundering have not been completely successful. The challenges faced in effective implementation of anti-money laundering efforts are following-

- **Fast pace of change in technology** including cyber technologies creates problems of tracking money launderers. The enforcement agencies have failed to match such a high rate of growth.
- **Predicate-offence-oriented law**: This means a case under the Act depends on the fate of cases pursued by primary agencies only such as the CBI, the Income Tax Department or the police. (Predicate offence- any offence that is component of more serious offence).
- **Lack of awareness about the seriousness** of Money Laundering in common people due to which they continue to use Hawala system offering fewer complexities and formalities.
- **Widespread act of smuggling**: There are a number of black market channels in India for the purpose of selling goods offering many imported consumers goods such as food items, electronics etc. which are routinely sold.
- **Failure of Banks to effectively implement KYC norms** as stipulated by the RBI.
- A number of black market channels sell **imported smuggled goods** and they deal in **cash transactions** and avoid custom duties thus generating black money.
- **Multiplicity of agencies** dealing with money laundering, cyber-crimes, terrorist crimes, economic offences etc. Such agencies **lack convergence** among themselves which is required to tackle multi-faceted and global nature of money laundering.
- Many **Tax Haven countries** exist which allows the creation of anonymous accounts with strict financial secrecy laws prohibiting the disclosure of financial information to foreign tax authorities.
- The provision of **financial confidentiality** in other countries which are unwilling in compromising with this confidentiality.

5. Way forward

- **Implement procedures for Anti Money Laundering provisions** as envisaged under the Prevention of Money laundering Act, 2002. Such procedures should include inter alia, the following three specific parameters which are related to the overall '**Client Due Diligence Process**:
  - Policy for acceptance of clients.
  - Procedure for identifying the clients.
  - Transaction monitoring and reporting especially suspicious transactions.
- **Role of bankers**: Bankers also has vital role and without their involvement, the operation cannot be successful.
- **Special cell dealing with money laundering activities**: It should be created on the lines of Economic Intelligence Council (EIC) exclusively dealing with research and development of anti-money laundering. This Special Cell should have link with INTERPOL and other international organizations dealing with money laundering. All key stakeholders, like, RBI, SEBI etc. should be a part of this.
- There is a requirement to have a convergence of **different enforcement agencies, sharing of information is necessary**.
- **Cryptocurrency and ML**: The following solutions could be implemented to tackle money laundering via cryptocurrency:
  - **AML procedures** can be strengthened at financial institutions;
  - **Transaction monitoring** can be enhanced and regulations can be improved. Regardless of the level of anonymity, criminals must exchange their cryptocurrency for fiat currency at some point. The monitoring of such transactions, within and across blockchains, can lead to the **de-anonymization** of criminals
  - **Third-party ID providers** can be placed under state supervision;
  - Cryptocurrency exchanges can be regulated, especially advanced digital exchanges and exchanges offering to purchase primary cryptocurrencies.
  - **Blockchain** can be used as a solution. A Blockchain-based platform will give regulators, auditors, and other stakeholders an effective and powerful set of tools to monitor complex transactions and immutably record the audit trail of suspicious transactions across the system.
- **Illegal Wildlife Trade and ML**
  - The FATF pointed out that following the money allows countries to identify a wider network of syndicate leaders and financiers involved, and to reduce the profitability of the crime.
  - Combating criminal organisations through their financial flows is a significant legal and investigative tool to prevent wildlife trafficking and the potential proliferation of zoonotic diseases.
  - To ensure the survival of endangered species, we need to build strong public-private partnerships to prevent, detect and disrupt this activity, following the money that fuels it and the organised crime gangs, poachers and traffickers behind it.
  - Estimating the proceeds of IWT to be between $7 and $23 billion per year globally, the FATF has suggested to all member governments that the financial aspect of wildlife trade needs to be looked at more carefully, and that money laundering laws should be applied to wildlife trade since the proceeds enters the global market through money laundering.

- The global nature of money laundering requires **international law enforcement cooperation** to effectively examine and accuse those that initiate these complex criminal organizations.
- Money laundering must be combated mainly by **penal ways** and within the frameworks of **international cooperation** among judicial and law enforcement authorities.
- There is a **need to draw a line** between financial confidentiality rules in various financial institutions and these institutions becoming money laundering havens.
- To have effective anti-money laundering measures there need to be a proper coordination between the Centre and the State. **The FATF Recommendations** set out a comprehensive and consistent framework of measures which countries should implement in order to combat money laundering and terrorist financing, as well as the financing of proliferation of weapons of mass destruction. Some of them are as
  - Identify the **risks**, and develop **policies** and domestic coordination.
  - Countries should criminalise money laundering on the basis of the **Vienna Convention and the Palermo Convention**. Countries should apply the crime of money laundering to all serious offences, with a view to including the widest range of predicate offences.
  - Countries should **implement targeted financial sanctions regimes** to comply with United Nations Security Council resolutions relating to the prevention and suppression of terrorism and terrorist financing.
  - Countries should **review the adequacy of laws and regulations** that relate to non-profit organisations which the country has identified as being vulnerable to terrorist financing abuse.
  - Apply **preventive measures** for the financial sector and other designated sectors.
  - Countries should ensure that **financial institution secrecy laws** do not inhibit implementation of the FATF Recommendations.
  - Financial institutions should be required **to maintain, for at least five years, all necessary records on transactions**, both domestic and international, to enable them to comply swiftly with information requests from the competent authorities.
  - Establish **powers and responsibilities** for the competent authorities (e.g., investigative, law enforcement and supervisory authorities) and other institutional measures.
  - Enhance the **transparency** and availability of **beneficial ownership information** of legal persons and arrangements.
  - **Facilitate international cooperation** to ensure that their competent authorities can rapidly, constructively and effectively provide the widest range of international cooperation in relation to money laundering, associated predicate offences and terrorist financing.

Therefore, to have an effective anti-money laundering regime, nations need to think regionally, nationally and globally to mitigate internal security threat associated with it.

6. UPSC Mains Previous Years' Questions

1. **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 counter-measures should be taken to prevent the same? (2018)**
2. **Money laundering poses a serious threat to country's economic sovereignty. What is its significance for India and what steps are required to be taken to control this menace? (2013).machine-based hosting for government businesses. (2015)**

7. Previous Years Vision IAS GS Mains Test Series Questions

1. Keeping in view the recent amendment, examine the efficacy of the Prevention of Money Laundering Act, 2002, in tackling the menace of money laundering in India.

Approach:

- Mention the recent changes in PMLA 2002.
- Briefly mention the significance of recent changes.
- Discuss efficacy of PMLA in the light of recent amendments.
- Highlight the issues in PMLA 2002.
- Conclude accordingly.

Answer:

PMLA 2002 was amended recently to define **politically exposed persons (PEPs),** lower the threshold for **beneficial ownership**, bring **crypto transactions** under its ambit and widen the ambit of reporting entities to incorporate **more disclosures for NGOs**. Further, the practicing **chartered accountants, company secretaries, and cost and works accountants** carrying out financial transactions on behalf of their clients are also brought into the ambit of this law.

The amendments assume significance ahead of India's **proposed FATF assessment**, which is expected to be undertaken later this year. These amendments will help enhance the efficacy of the PMLA 2002 in following manner:

- It expands the scope of the act by including **financial professionals** for reporting transactions on behalf of their individual clients. It is expected to aid investigative agencies further in their probe against dubious transactions involving shell companies and money laundering.
- Definition of politically exposed persons under PMLA brings **uniformity with Reserve Bank of India's (RBI)** KYC norms/anti-money laundering standards for banks and financial institutions.
- **Lowering the threshold** for beneficial ownership, from 25% to 10% ownership in company, will help bring more indirect participants within the reporting net.
- The necessary **due diligence documentation** has now expanded beyond just getting the fundamental KYCs of clients to include submission of details such as names of persons holding senior management positions, names of partners, names of beneficiaries, trustees, settlers and authors etc.
- Intermediaries operating in the crypto ecosystem such as **crypto exchanges, wallets, and other service providers** will need to implement PMLA controls and systems such as KYC checks, monitor and report suspicious transactions and have policies in place for transaction tracing.

Though the scope of PMLA 2002 has been widened to make it more effective, it suffers from some lacunae such as:

- **List of schedule offences under PMLA 2002** has been expanded considerably. The inclusion of **non-serious offences** may dilute the objective of the PMLA. For example, **search or raid was conducted by ED in only 8.99% of the cases out of the total 5,906 ECIRs** filed till now.
- Since its inception in 2005, **trials have been completed in only 25 cases** and it is under progress in another 1142 cases. This happens because most accused under this law are affluent and they use legal loopholes to obtain adjournments and delay the conviction process.

- **Excessive powers provided to ED** under the Act with respect to stringent bail conditions, lack of transparency in Enforcement Case Information Report (ECIR), ED's power to attach the assets under PMLA may lead to its misuse. For example, the opposition has complained that ED probes are launched for political reasons.

The objective of this law is to prevent money laundering. In order to achieve this objective, some far-reaching powers are essential. However, these powers should be used only for legitimate purposes and checks and balances should be maintained to prevent the misuse of these powers.

2. Establishing linkages between globalisation and money laundering, discuss the initiatives taken at the national and international levels to combat it.

Approach:

- Introduce by highlighting the meaning of money laundering and globalisation.
- Explain the relationship between globalisation and money laundering.
- Enlist the measures taken at national and global level to combat money laundering.
- Conclude accordingly.

Answer:

Money laundering is the process of concealing the source of money obtained illegally by passing it through a complex sequence of transfers or commercial transactions. While globalisation is the process where the world is becoming increasingly interconnected as a result of massively increased trade and cultural exchange.

Linkages between globalisation and money laundering:

- The growth in international trade, the expansion of the global financial system, the lowering of barriers to international travel, and the surge in the internalization of organized crime have combined to **provide the source, opportunity, and means** for converting illegal proceeds into what appears to be legitimate funds.
- The **deeper "dirty money" gets into the international banking system**, the clandestine nature of money-laundering makes it difficult to estimate its origin.
- The number of **developments in the international financial system** during recent decades have made the three **F's - finding, freezing and forfeiting** of criminally derived income and assets all the more difficult.
- These developments include "dollarization" of black markets, the general trend towards **financial deregulation, the progress of the Euro market and the proliferation of financial havens**.
- Fuelled by advances in technology and communications, the financial infrastructure has developed into a perpetually operating global system in which "**megabyte money**" (i.e. money in the form of symbols on computer screens) can move anywhere in the world with speed and ease.
- Rapid developments in financial information, technology and communication **allow money to move anywhere in the world with speed and ease**.

Faced with the above challenges, following efforts have taken:

At the international level:

- **The Vienna Convention**: It promotes **international cooperation in investigations and makes extradition between member states** applicable to money laundering.

- **The Financial Action Task Force (FATF)**: It helps to build the **capacity to fight terrorism and trace terrorist money and to successfully investigate and prosecute** money laundering and terrorist financing offences.
- **Basel Committee's Statement of Principles**: It seeks to **deny the banking system to those involved in money laundering** by the application of the four basic principles namely, identifying the customer, compliance with the laws, cooperation with Law Enforcement Agencies and adherence to the Statement.

At the national level:

- **Prevention of Money-laundering Act, 2002**: The Act and Rules impose obligation on banking companies, financial institutions and seeks to prevent and control money laundering, confiscate and seize the property obtained from the laundered money.
- **Financial Intelligence Unit**: It receives financial information pursuant to country's anti-money laundering laws; analyses, processes and disseminates it to appropriate national and international authorities, to support anti-money laundering efforts.
- **The Black Money (undisclosed foreign income and assets) and Imposition of Tax Act, 2015**: To deal with the menace of the black money existing in the form of undisclosed foreign income and assets by setting out the procedure for dealing with such income and assets.
- **Benami Transactions (Prohibition) Amendment Bill, 2015**: It aims to expand the definition of Benami Transactions and specifies the penalty to be imposed on a person entering into a Benami transaction.
- **Anti-money laundering/counter financing of terrorism–guidelines for general insurers, 2013**: Each insurance company has to establish and implement policies, procedures, and internal controls/ audit in its AML/CFT program. Insurers are also required to maintain records of their transactions under these guidelines.

Money laundering has become a quintessential problem and combating it has become an international priority. The efforts such as increasing financial literacy, promoting KYC norms and cashless digital transactions etc. are additional steps in the right direction to tackle money laundering.

3. Any counter-terrorism strategy can succeed only if sources of terrorist funding are blocked by efficient financial regulation. In light of the statement discuss the need for an efficient legal framework to combat terror financing in India and steps taken by the government in this regard.

Approach:

- Question must be answered in two parts
- Stress on the need for legal framework to tackle terrorist financing.
- Enumerate the steps taken by government to block the financing routes.

Answer:

Terrorism finance (TF) has been termed as the lifeblood of terrorism, one of the most important factors sustaining its continuing threat, both from within and without.

Need for legal framework to combat terrorist financing-:

- **Prevention and early detection** is at the core of government threat mitigation efforts. Preventing terrorists from raising, moving, placing and using funds is central to this effort. Government must deprive terrorists of their enabling means, which includes financial support, by expanding and enhancing efforts aimed at blocking the flow of financial resources to and among terrorist groups and to disrupt terrorist facilitation and support activities, pursuing prosecutions to enforce violations and dissuade others.

- **Efficient legal framework** helps in checking activities that generate funds for terrorist activities like drug trafficking, human trafficking, arms smuggling and range of the activities. In India we have numerous legal instruments to block the sources. Prevention of Money Laundering Act, 2002 (PMLA), the Narcotic Drugs and Psychotropic Substances Act, 1985 (NDPS Act) and Unlawful Activities (Prevention) Act, 1967 (UAPA) are some of the legislations that are aimed at blocking the activities that produce funds for terrorist activities.
- The **Financial Intelligence Unit, India (FIU-IND)**, as an independent body is responsible for coordinating and strengthening efforts of national and international intelligence, investigation and enforcement agencies in pursuing the global effort against money laundering, terrorist financing and related crimes. They need Protection from criminal and civil proceedings for breach of restrictions and disclosure of the information during investigation.

Steps taken by Government:

- India has joined as the **34th member of Financial Action Task Force (FATF)**. FATF membership is important as it will help India to build the capacity to fight terrorism and trace terror funds and to successfully investigate and prosecute money laundering and terrorist financing offences.
- **PMLA** has been amended in 2013 to overcome the difficulties being faced in its enforcement and to conform to international standards. The definition of money laundering has been expanded, new category entities is created to include non-financial businesses. Sanctions are substantially increased in the amended act along with the removal of upper limit on the fine.
- Amended act provides **empowers the FIU** to seek compliance to the PMLA and greater protection during investigation of cases.
- **UAPA Act amended in 2013**, adds to the efficiency of existing framework and meets standards set by FATF. Amended act terms production smuggling and circulation of counterfeit currency as terrorist act. It expands the ambit of act by including companies, trusts and societies for investigation.

India's serious commitment to combating terrorism in all its forms is acknowledged internationally. From a law enforcement perspective, this commitment is reflected in an active pursuit of the financial aspects of terrorism.

4. India has put in place stringent rules to tackle money laundering. The growing challenge is compliance to the Anti-Money Laundering legislations. What are the various constraints in compliance to legislations?

Approach:

Briefly explain the Anti-Money Laundering (AML) framework in India.

Enumerate the constraints in the given framework to tackle money laundering.

Answer:

Money Laundering is a global phenomenon being employed by launderers worldwide to conceal criminal activities associated with it such as drugs, arms, human trafficking, terrorism and extortion, smuggling, financial frauds, corruption etc.

The **Financial Intelligence Unit - India (FIU-India)** is the nodal agency in India for managing the AML ecosystem and has significantly helped in coordinating and strengthening efforts of national and international intelligence, investigation and enforcement agencies in pursuing the global efforts against money laundering and related crimes; while the Prevention of Money Laundering Act (PMLA), forms the core framework for combating money laundering in the country.

There are many **key constraints** which need to be addressed to implement an effective AML regime in India. Some of the key constraints are as follows:

- Unlike relatively mature regulatory countries, Indian AML regulations are being **viewed as a compliance tool** by the financial services community rather than as a risk management tool. Hence the objective has been basic compliance rather than using it as a risk management practice.
- **Lack of adequate number of skilled and certified AML workforce** is also a big operational challenge. Unawareness about the grave problem of money-laundering among the common people and dealing staff is also an impediment in having a proper AML regime.
- AML compliance brings a **huge financial burden** on the financial institution. To keep up with the regulatory environment, sound investments are required in customer due diligence, customer identification and acceptance procedures, monitoring suspicious transactions and related AML processes and procedures.
- **Absence of comprehensive enforcement agency** to tackle exclusively cases of money-laundering. Separate wings of various law enforcement agencies are dealing with digital crimes, money laundering, economic offences and terrorist crimes. These agencies lack convergence on matters of money-laundering. The Special Investigation Team (SIT) on black money recommended an integrated system of investigations into black money.
- **Technical shortcomings** in the **criminalisation** of both money laundering and terrorist financing and in the domestic framework of confiscation and provisional measures.
- Despite all available infrastructures through government bodies, the **onus of AML implementation mostly lies with financial institutions**. Most institutions see it as a financial and operational burden. Depending on the size and different lines of business for a given financial institution, the scope of a given AML programme can vary significantly. A lack of clarity over compliance and tighter timelines can result in ad hoc implementation of AML processes rather than a long-term, strategic solution.
- Another significant issue is **lack of enforcement**. Despite the laws that criminalise money laundering and empower authorities to confiscate assets, prosecutions and convictions have been few and the rate of confiscation is low. Based on the findings, the SIT has recommended to the government stricter enforcement of tax laws and expediting pending prosecutions. Government records revealed that over 8,000 prosecution cases pertaining to direct tax laws had been pending for the past several years. Nearly 5,000 other cases had been pending before lower courts for over a decade in Mumbai alone.

India has a long way to go before we can match the efforts of developed countries in the area of AML. The government needs to take more effective action and generate a grassroots-level focus amongst financial institutions. It is difficult to implement control over money laundering activities without support from legislative and executive bodies.

5. What are the various factors which make India vulnerable to the menace of Money Laundering activities? Discuss some international efforts which have been taken in this regard.

Approach:

- First define Money Laundering. Then point wise discuss the factors why India is vulnerable to laundering. Talk about international organizations and actions/initiatives taken by different countries

Answer:

Money laundering involves disguising financial assets so that they can be used without detection of the illegal activity that produced them. It is a process by which illegal money generated is legalized using various instruments. It comprises of three aspects – layering, placement and integration

The Prevention of Money Laundering Act, 2002 (PMLA) forms the core of the legal framework put in place by India to combat money laundering. Money can be laundered by many methods, which vary in complexity and sophistication.

Out of 140 countries India was ranked 70th in 2013 Anti money laundering basal level which clearly shows that our economy is very vulnerable to money laundering activities. The recent activity in money laundering in India is through political parties, corporate companies and the shares market. It is investigated by the Enforcement Directorate and Indian Income Tax Department. According to Government of India, out of the total tax arrears of INR2480 billion (US$40 billion) about INR1300 billion (US$21 billion) pertains to money laundering and securities scam cases.

Some common sources of illegal proceeds in India are narcotics trafficking, trade in illegal gems (particularly diamonds), smuggling, trafficking in persons, corruption, and Income-Tax evasion

Large portions of illegal proceeds are laundered through the alternative remittance system called "hawala" or "hundi" (estimated to account for up to 30 per cent of India's GNP)

Under this system, individuals transfer funds or other items of value from one country to another, often without the actual movement of currency. The system provides anonymity and security; permits individuals to convert currency into other currencies; lets them convert narcotics, gold, or trade items into currency.

Historically, gold has been one of the most important instruments involved in Indian hawala transactions. There is a widespread cultural demand for gold in the region.

People prefer to avoid the lengthy paperwork required to complete a money transfer through a financial institution and hawala dealers can provide the same service with little or no documentation and at rates less than that charged by banks.

In recent years, it is believed that the growing Indian diamond trade has also been increasingly important in providing counter evaluation or a method of "balancing the books" in external hawala transactions.

It is often very difficult for competent authorities to identify the natural, real person who truly has ownership and control of a company, trust or other corporate vehicle, particularly when the arrangement involves several countries

The processes by which criminally derived property may be laundered are extensive. Though criminal money may be successfully laundered without the assistance of the financial sector, the reality is that hundreds of billions of dollars of criminally derived money is laundered through financial institutions, annually. The nature of the services and products offered by the financial services industry (namely managing, controlling and possessing money and property belonging to others) means that it is vulnerable to abuse by money launderers.

Following are the international efforts taken in this regard are:

- Many regulatory and governmental authorities issue estimates each year for the amount of money laundered, either worldwide or within their national economy.
- The Financial Action Task Force on Money Laundering (FATF), an intergovernmental body set up to combat money laundering. FATF sets global standards for Anti Money Laundering and Countering Financing of Terrorism (AML/CFT) regulations for governments across the world, while India has been its member since 2010.
- The 1988 United Nations Convention against the Illicit Traffic in Narcotic Drugs and Psychotropic Substances is the first international legal instrument to embody the money-laundering aspect of this new strategy and is also the first international convention, which criminalizes money-laundering.
- In September 2003 and December 2005, the UN Convention against Transnational Organized Crime and the UN Convention against Corruption respectively came into force. Both instruments widen the scope of the money-laundering offence by stating that it should not only apply to the proceeds of illicit drug trafficking, but should also cover the proceeds of all serious crimes. Both Conventions urge States to create a comprehensive domestic supervisory and regulatory regime for banks and non-bank financial institutions, including natural and legal persons, as well as any

entities particularly susceptible to being involved in a money-laundering scheme. The Conventions also call for the establishment of Financial Intelligence Units (FIUs).

- Multilateral fora other than the Financial Action Task Force like the Eurasian Group on Combating Money Laundering and Financing of Terrorism, and the Asia Pacific Group on Money Laundering (APG) also need to be optimally utilized by the Enforcement Directorate for bilateral exchanges and follow up with counterpart enforcement agencies for better mutual cooperation.
- Recently a coordinated international effort to disrupt a sophisticated transnational money laundering network resulted in 13 searches conducted across Australia, with a further nine search warrants conducted by Indian Enforcement Directorate in India.

6. Money laundering and terrorism have strong inter-linkages. Illustrate. In this context, how far do the steps taken by the government confirm with the international commitments?

Approach:

- Show the 'supply-chain' of terror and money laundering.
- The next part has to discuss some measures taken by Indian government to combat money laundering and their performance.
- The next part may discuss some corrective measures to make them more effective.

Answer:

Money laundering and terrorism financing may be seen as distinct activities, but they are generally inter-related. Both often display similar transactional features, mostly having to do with concealment. Money launderers send illicit funds through legal channels so as to conceal their criminal origins, while those who finance terrorism transfer funds that may be legal or illicit in origin in such a way as to conceal their source and ultimate use, which is the support of terrorism. The techniques used to conceal the sources/ end-uses normally involve multiple financial institutions, shell companies, carriers, etc.

If the source can be concealed, it remains available for future terrorist financing activities. Similarly, it is important for terrorists to conceal the use of the funds so that the financing activity goes undetected. The mesh of the intermediaries helps in creating bloated values and facilitates diversion of actual wealth to terrorist sources.

The two activities often have convergent interests:

- Criminal organizations benefit from the ability of terrorist organizations to do damage, while the latter in turn benefit from the financing that criminal activities can obtain for them.
- Ideology can become the front for organized crime. For example, in pre-2009 Sri Lanka, Chechaniya etc.
- Front end activities like religious NGOs act as a conduit to get illicit money via donations and divert them for terrorist activities. Prominent example is Hafeez Sayeed.

Thus, money laundering can not only lead to economic offence but may also be a threat to international peace and security. As a result, there have been many international initiatives to curb the menace of money laundering. Some of these are:

- The 1988 Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances: It combats drug trafficking organizations by emphasizing attacking the goal of all organized crime, and also its weakest point namely money itself.
- The United Nations Convention against Transnational Organized Crime: It is designed to combat the phenomenon of transnational organized crime.

- Financial Action Task Force on Money Laundering (FATF): It is an intergovernmental body established in 1989 and is responsible for setting global standards on anti-money laundering and combating financing of terrorism. At present, it is the most comprehensive mechanism to deal with money laundering with 40 recommendations. It seeks to achieve three objectives: combating money laundering; strengthening financial system; and international cooperation.
- India has been classified as high risk zone in terms of money laundering. Out of 140 countries, India was ranked 70th in 2013 by the Anti Money Laundering (AML) Basel Index.

This clearly shows that India, is vulnerable to money laundering activities. To counter these threats, India became a member of the Financial Action Task Force in 2010. India is also a signatory to various international Conventions on anti-money laundering and countering financing of terrorism. These measures include:

- The Income Tax Act, 1961.
- The Benami Transactions (Prohibition) Act, 1988, amended recently.
- The Indian Penal Code and Code of Criminal Procedure, 1973.
- The Narcotic Drugs and Psychotropic Substances Act, 1985.

However, they proved to be inadequate. Therefore, the Prevention of Money Laundering Act (PMLA) was passed in 2003. Later, (PMLA) was amended many times making money laundering a criminal offence and the ambit of PMLA has been widened by a recent amendment.

Recently, government agencies have launched a massive National Risk Assessment (NRA) exercise to identify the sectors that are susceptible to money laundering and terror funding, and plug the loopholes. This is in line with the Financial Action Task Force (FATF) recommendations.

7. Money Laundering as a socio economic offence is a menace especially for developing countries like India. Comment. What measures have been taken at the domestic and international levels to deal with this menace?

Approach:

- Briefly introduce by explaining what is money laundering.
- Discuss how it is a socio-economic menace especially for developing countries like India.
- Enumerate the measures at the national level as well as the global level to deal with money laundering.
- Give brief conclusion.

Answer:

Money Laundering is the method by which criminals disguise the illegal origins of their wealth and protect their asset bases, so as to avoid the suspicion of law enforcement agencies and prevent leaving a trail of incriminating evidence. It is done through various measures such as misinvoicing of trade, using tax havens, shell companies etc. According to estimates by an IMF study, the quantum of money laundered is approximately 2-5 % of global GDP.

Money laundering as a socio-economic offence:

- **Weakens social fabric**: Money laundering gives impetus to criminal activities, like smuggling, corruption, drug trafficking, tax evasion, insider trading etc. and leads to deterioration of collective ethical standards, threatening the peace and prosperity of the society.
- **Undermines democracy and rule of law**: It transfers purchasing power and market dominance in the hands of the criminal elements which can acquire control of large sectors of the economy through investment, or offer bribes to public officials and governments.

- **Undermines welfarism**: Laundering for reasons such as tax evasion leads to diversion of the resources, which could have been used by the government to further the implementation of welfare schemes for citizens.
- **Affects economy and its development**: It undermines the integrity of the financial markets of the nation and the associated criminal activities leads to loss of revenue, economic distortion and instability in the market. The perception of increased risk also keeps investors at distance.

It is a **menace especially for developing countries** like India as:

- Developing countries are more exposed and vulnerable to exploits of money laundering due to lax regulatory and legal environment, lack of transparency, weak corporate governance and vulnerable financial systems along with persistent civil and political unrest - a common feature of developing countries.
- **Social evil of poverty** also makes the population susceptible to laundering activities.
- Further, the government has an **enhanced burden to ensure productivity** for its impoverished by diversion of precious resources. Illicit flows reduce the chances of success of these domestic resource mobilization initiatives.

Since money laundering is not only a law enforcement problem but a serious national and international security threat, various actions have been taken at both the levels.

At National level

- **Legislative measures**: Enactment of anti-money laundering laws like prevention of money laundering Act 2002 (amended in 2012) to help financial institutions in protecting our economy as well as acts such as Black Money Act, 2015, Benami Transactions Act, Foreign exchange management Act etc.
- **Establishment of various regulators and enforcement agencies** such as Financial Intelligence Unit, Directorate of Enforcement etc.
- **Transparency norms**: RBI has introduced stricter KYC norms and also made it applicable for mobile wallets etc.
- **International agreements**: The Government of India has entered into Double Taxation Avoidance Agreements (DTAAs), to enable exchange of information pertaining to money laundering as well as Advanced Pricing Agreements to avoid tax evasion and generation of black money.
- **Strict monitoring by SEBI**: The Foreign Portfolio Investors (FPIs) which issue Participatory Notes need to follow stricter norms of monthly reporting.

At Global level

- **Blacklisting of countries** by Financial Action Task Force, which it judges to be non-cooperative in the global fight against money laundering and terrorist financing.
- **Automatic Exchange of Financial Information** by many countries as part of the OECD initiative.
- **Base Erosion and Profit Shifting (BEPS) initiative**, under which the countries have agreed to take necessary measures, requiring their large MNCs to provide reporting on revenues, profits, losses, sales, taxes paid etc.
- **United Nations Convention against Illicit Trafficking in Drugs and Psychotropic Substances** also known as Vienna Convention requires States to establish money laundering as a criminal offence.

To combat the menace of money laundering, other measures such as introduction of plastic money, sensitization of the masses about the nuances of the crime for early detection of the crime can be undertaken to prevent its adverse effect on the socio-economic growth of the country.

8. Money laundering not only threatens the stability of the financial system of India but also its national security. Elucidate. In this context, discuss how far the Prevention of Money Laundering Act, 2002 addresses these issues.

Approach:

- Give a brief definition of money laundering.
- Discuss how it threatens stability of financial system of India.
- Discuss how it affects the national security.
- Then discuss how PMLA, 2002 has addressed these issues.
- Further discuss the shortcomings or issues with the Act in brief and conclude.

Answer:

Money laundering is the process of making large amounts of money generated by a criminal activity, such as drug trafficking or terrorist funding, appear to have come from a legitimate source. It presents a tool for criminal organizations in using illegally obtained money effectively.

It threatens the stability of the financial system of India in following ways:

- **Undermining legitimate private sector**: Criminals use front companies to launder illicit funds and their ability to draw on these excess funds enables them to "subsidize" their products, offering them at below market levels making it difficult for the legitimate firms to compete.
- **Impacts integrity of financial markets**: Movement of large sums of cash, via wire transfers, suddenly and without notification, causing liquidity problems and possible bank runs.
- **Compromises economic policy**: Money laundering distorts money demand and creates volatility in global capital flows as well as interest and exchange rates, thereby disturbing any attempt to establish beneficial economic policy.
- **Loss of government revenue**: Criminal proceeds are hidden to escape detection, thus, governments are unable to tax the funds, causing governments to lose revenue.

Further money laundering activities also impact national security in following ways:

- **Induces criminal activities**: Money laundering is often associated with the illegal activities of the organized crime (drug trafficking, arms dealings, terrorism, human trafficking, etc.) impacting security of a nation.
- **Increasing security costs**: Expansion of criminal operations drives up the security cost of government.
- **Political instability**: It helps criminals accrue huge economic clout, which has a corrupting effect on all elements of society. In extreme cases, it can lead to the virtual take-over of legitimate government.

In this context, the government introduced Prevention of Money Laundering Act, 2002 to counter money laundering. It has brought following advancements in anti-money laundering regime in India:

- **Maintenance of records**: Every reporting entity needs to maintain a record of all transactions in such a manner that it enables to reconstruct individual transactions.
- **Confiscation of assets**: The property obtained by proceeds of crime, even when transferred out of the country, can be attached provisionally during the investigation or permanently after conviction.
- **Institutional development**: The Enforcement Directorate in the Department of Revenue, Ministry of Finance is empowered to investigate the cases of money laundering under the PMLA.

- **Speedy trial**: It provides for expeditious trial through special courts.
- **Wide ambit**: It provides for investigation and prosecution of accomplice family members of an offender in money laundering case.

It has managed to sniff out over Rs. 9,000 crore as suspected haul from money laundering in a decade. However, **PMLA has been successful only partially** in achieving its objectives.

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

Approach:

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

Answer:

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

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

Costs of money laundering

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

Necessity of trans-national cooperation

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

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

Initiatives taken by global community

- **Financial Action Task Force (FATF)**: It is an inter-governmental body that sets standards and promotes effective implementation of legal, regulatory and operational measures to combat money laundering and terrorist financing and other related threats to the integrity of the international financial system.
- **Asia Pacific group**: It works with countries in the Asia-Pacific to generate wide regional commitment to implement anti-money laundering policies and initiatives and secure agreement to establish a more permanent regional anti-money laundering body.
- **Basel Committee on Banking Regulations and Supervisory Practices** issued a statement of principles to ensure that banks are not used to hide or launder funds acquired through criminal activities.
- **Various international conventions** are also established to prevent money laundering such as the United Nation Convention against Transnational Organised Crime (2000) among others.
- **Tax treaties** that facilitate and enhance exchange of information under the Tax Treaties e.g. India's Foreign Account Tax Compliance Act with the US.
- **The Multilateral Competent Authority Agreement** (MCAA) is also developed for Automatic Exchange of Information as per Common Reporting Standards (CRS).

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

Heartiest Congratulations to all Successful Candidates

Aditya Srivastava

16 in **TOP 20** Selections in **CSE 2023** from various programs of **Vision IAS**

Animesh Pradhan

Ruhani

Srishti Dabas

Anmol

Nausheen

Aishwaryam Prajapati

39 Selections in **TOP 50** in **CSE 2022**

Ishita Kishore

Garima Lohia

Uma Harathi N

1 AIR

SHUBHAM KUMAR

CIVIL SERVICES EXAMINATION 2020

DELHI

HEAD OFFICE
Apsara Arcade, 1/8-B 1st Floor, Near Gate-6 Karol Bagh Metro Station

MUKHERJEE NAGAR CENTER
Plot No. 857, Ground Floor, Mukherjee Nagar, Opposite Punjab & Sindh Bank, Mukherjee Nagar

GTB NAGAR CENTER
Classroom & Enquiry Office, above Gate No. 2, GTB Nagar Metro Building, Delhi - 110009

FOR DETAILED ENQUIRY
Please Call:
+91 8468022022,
+91 9019066066

enquiry@visionias.in /c/VisionIASdelhi /visionias.upsc /vision _ias VisionIAS_UPSC

AHMEDABAD BENGALURU BHOPAL CHANDIGARH DELHI GUWAHATI HYDERABAD JAIPUR JODHPUR LUCKNOW PRAYAGRAJ PUNE RANCHI

VISIONIAS
INSPIRING INNOVATION

CLASSROOM STUDY MATERIAL

Internal Security

BASICS OF CYBER SECURITY

CONTENTS

1. Introduction to Cyber Security

As per **Information Technology Act, 2000,** "Cyber security means protecting information, equipment, devices computer, computer resource, communication device and information stored therein from unauthorised access, use, disclosure, disruption, modification or destruction."

According to EY's latest Global Information Safety report, India has one of the highest number of cyber attacks and the country ranks second in terms of targeted attacks.

1.1. Cyberspace

India's Cyber Security Policy 2013 defines cyberspace as a complex environment comprising **interaction between people, software and services,** supported by worldwide distribution of information and communication technology devices and networks.

It is a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the internet, telecommunications networks, computer systems and embedded processors and controllers.

1.2. Cyberthreats

Cyberthreats can be disaggregated into **four baskets** based on the perpetrators and their motives - Cyber **Espionage,** Cyber **Crime,** Cyber **Terrorism,** Cyber **Warfare.**

1.2.1. Cyber Crime/ Cyber Attacks

Cyber-attack is "any type of **offensive maneuver** employed by individuals or whole organizations that targets computer information systems, infrastructures, computer networks with an **intention to damage or destroy** targeted computer network or system."

These attacks can be labeled either as Cyber-campaign, Cyber-warfare or Cyber-terrorism depending upon the context, scale and severity of attacks. Cyber-attacks can range from installing spyware on a PC to attempts to destroy the critical infrastructure of entire nations.

1.2.2. Cyber terrorism

The acts of terrorism related to cyber space or executed using cyber technologies is popularly known as 'cyber terrorism'.

> *"Cyber terrorism is the convergence of terrorism and cyber space. It means unlawful attacks and threats of attacks against computers, networks, and information stored to intimidate or coerce a government or its people to further political or social objectives. . Further, 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."*

It should be noted here that if they create panic by attacking critical systems/infrastructure, there is no need for it to lead to violence. In fact, such attacks can be more dangerous.

Besides, terrorists also use cyberspace for purposes like planning terrorist attacks, recruiting sympathizers, communication purposes, command and control, spreading propaganda in form of malicious content online for brainwashing, funding purposes etc. It is also used as a **new arena for attacks** in pursuit of the terrorists' political and social objectives.

1.2.3. Cyber warfare

Cyber warfare is defined as, "The use of computer technology to disrupt the activities of a state or organization, especially the deliberate attacking of information systems for strategic or military purposes." These hostile actions against a computer system or network can take any form. On one hand, it may be conducted with the smallest possible intervention that allows extraction of the information sought without disturbing the normal functioning of a computer system or network. This type of intervention is never noticed by the user and happens on a continuous basis. Other type may be destructive in nature which alters, disrupts, degrades, or destroy an adversary's computer systems.

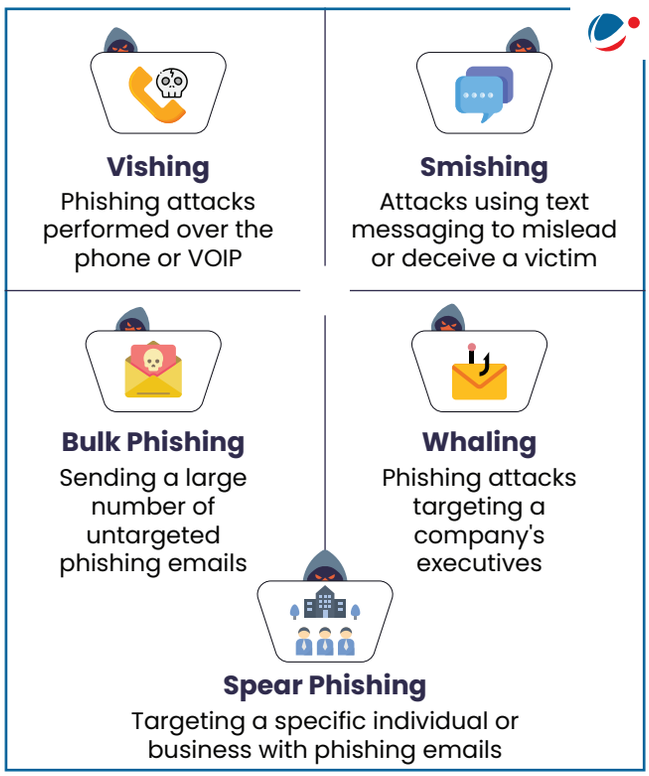
1.2.4. Cyber Espionage

Cyber espionage is defined as, "The use of computer networks to gain illicit access to confidential information, typically that held by a government or other organization." It is generally associated with intelligence gathering, data theft and, more recently, with analysis of public activity on social networking sites like Facebook and Twitter. These activities could be by criminals, terrorists or nations as part of normal information gathering or security monitoring.

Examples of Cyber Espionage include- 2014 hacking of major US companies to steal trade secrets by Chinese officials; Titan Rain; Moonlight Maze; NSA surveillance Program as revealed by Edward Snowden in USA.

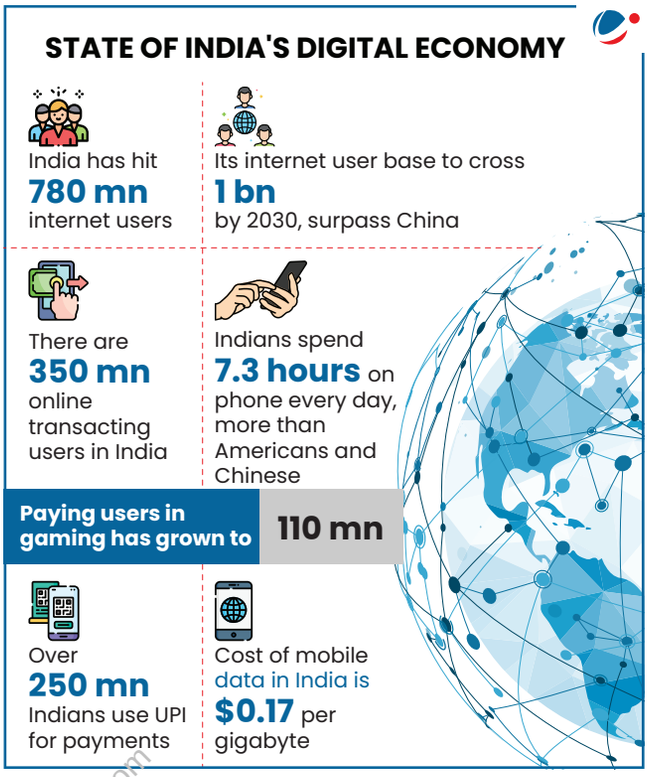
1.2.5. Main Cyber players and their motives

- **Cyber Criminals:** Seeking commercial gain from hacking banks and financial institutions as well as phishing scams and computer ransomware.
- Phishing is a broad term for cyberattacks that use social engineering to trick victims into paying money, handing over sensitive information, or downloading malware.
- **Cyber Terrorists** with the mission to penetrate and attack critical assets, and national infrastructure for aims relating to political power and "branding".
- **Cyber Espionage:** Using stealthy IT malware to penetrate both corporate and military data-servers in order to obtain plans and intelligence.
- **Cyber Hacktivists:** Groups such as "Anonymous" with political agendas that hack sites and servers to virally communicate the "message" for specific campaigns.



1.3. Importance of Cyberspace

Cyber Security has assumed strategic and critical importance because of following reasons:



- Cyberspace has become a key **component** in the formulation and execution of public policies such as move towards digital India, payment infrastructure, etc.
- It is used by the government to process and store **sensitive and critical data** which if compromised can have devastating impact. The successful implementation of Aadhaar highlights the importance of cyberspace in public service delivery mechanism.
- Taking down cyberspace will result in **disruption of many critical public services** like- railways, defense systems, communication system, banking and other financial systems etc.
- Several **states are developing the capabilities** in the area of cyberattacks which can alter outcomes in the battlefield.
- **Individuals** are using internet based services at a growing pace making them vulnerable to cybercrimes, such as- online bank frauds, surveillance, profiling, violation of privacy etc. The recent push towards work from home due to the pandemic has increased the dependence of individuals on cyberspace.

1.4. Challenges in Defending Cyberspace

The task of tackling cyber-attacks is more difficult than conventional threats due to following reasons

- **Diffused and intangible threat** in the absence of tangible perpetrators coupled with low costs of mounting an attack makes it difficult to frame an adequate response.
- **Difficult to locate** the attacker who can even mislead the target into believing that the attack has come from somewhere else.
- **Absence of any geographical constraints** enabling attackers to launch attack anywhere on the globe.
- **Need for international cooperation -** Cyberspace is inherently international even from the perspective of national interest. It is not possible for a country to ignore what is happening in any part of this space if it is to protect the functionality of the cyberspace relevant for its own nationals.
- **Rapidly evolving technology** needs investment, manpower and an ecosystem to keep track of global developments, developing countermeasures and staying ahead of the competition.
- **Non-existence of foolproof security architecture** due to low resources requirement for attackers to launch attacks coupled with potential bugs in any system.

- **Human element in cybersecurity –** Target users, themselves, make mistakes and fall prey to cyberattack. Most sophisticated cyberattacks have all involved a human element: Stuxnet needed the physical introduction of infected USB devices into Iran's nuclear facilities; the 2016 cyber-heist of $950 million from Bangladesh involved gullible (or complicit) bankers handing over SWIFT codes to hackers.

Challenges are increasing in the Cyber Space Domain

Attacks	Targets	Effects
Insider Attack Unwitting Behaviour	Human Organisation	Disinformation, Distraction, Confusion
Data and Policy Corruption	Space Mission layer	Disruption of Command & Control, behavioural manipulation
Code Manipulation, Malware	Application layer	Induced inaccuracies and failures
Worms, Viruses flooding	Operating System/ Network layer	Denial of Services, exfiltration
Lifecycle implants of backdoors	Hardware Systems Layer	Triggered malfunction, performance loss
Physical destruction eavesdropping	Materials, Devices and Commn. Links	Loss of Communication

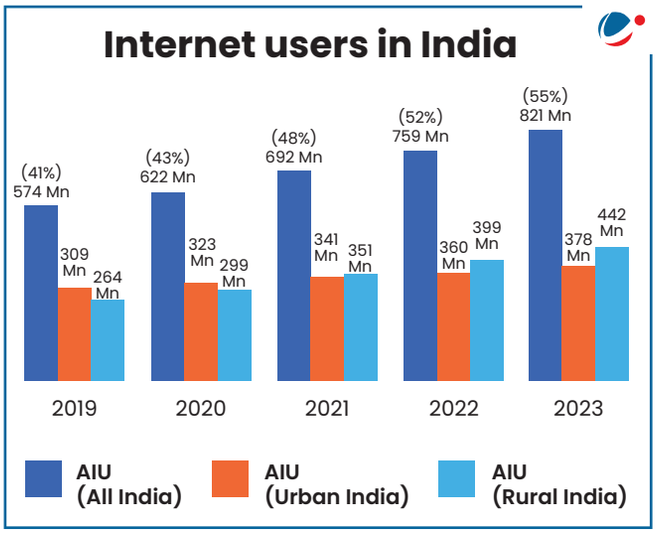
Net-centricity and interoperability increase the risk of cyber-attacks
Software is the most apparent target of cyber- attacks, especially when plagued with a lack of quality, questionable pedigree and uncontrolled access to development environments

Mitigation is a challenge - it requires:
- Development Environment access control
- Architectural considerations
- Technology and tools
- Informed operator responsiveness

2. Cybersecurity in India

India has more than 820 million active internet users at present. Over half of them — 442 million — now come from rural parts of the country. In 2023, internet penetration grew eight per cent year-on-year. India's internet user base is to cross 1 billion by 2030 and surpass China.

The pace of growth of internet usage is pushing us towards a **digital society** and the government itself has rolled out various programs for digitization of India, e.g.- Digital India Program.



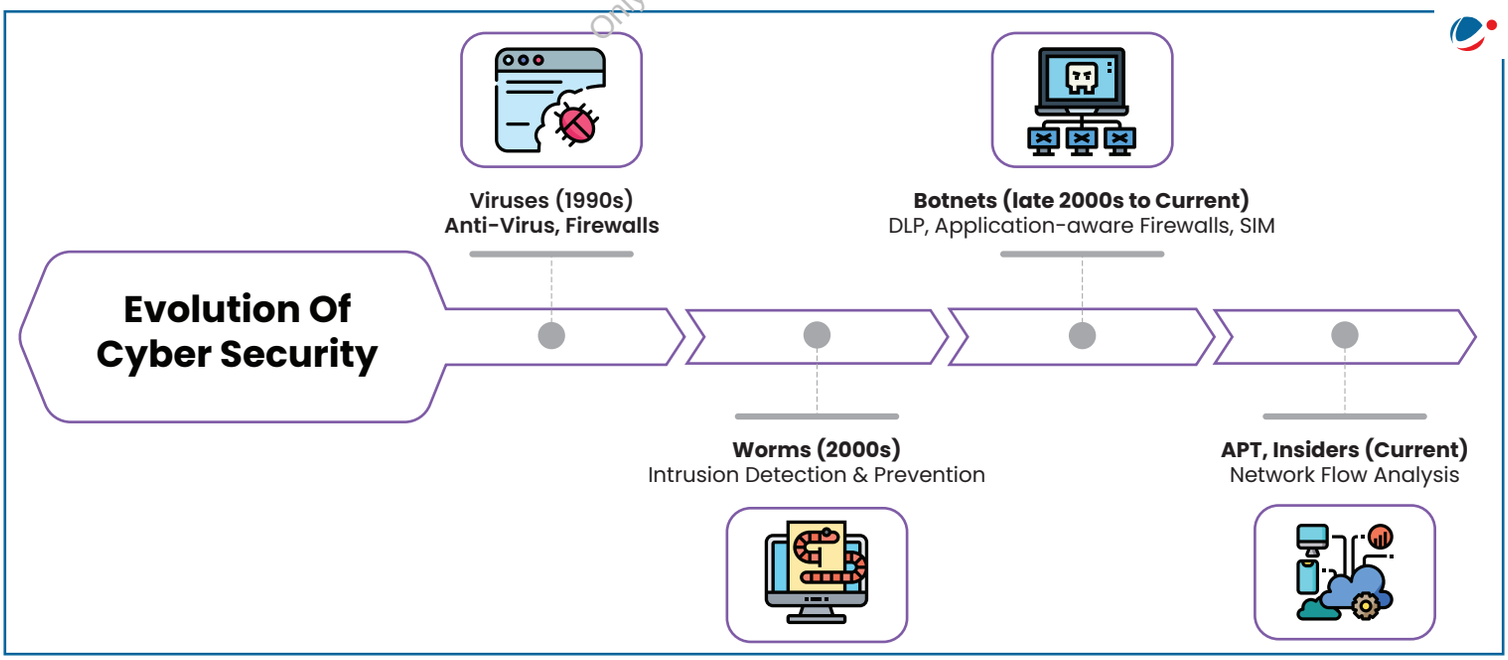
2.1. Current Situation

According to National Crime Records Bureau (NCRB), India saw a rise of 24 per cent in cybercrimes registered in 2022 compared to 2021. During 2022, 64.8 per cent of cybercrime cases registered were for the motive of fraud – 42,710 out of 65,893 cases – followed by extortion with 5.5 per cent – 3,648 cases – and sexual exploitation with 5.2 per cent – 3,434 cases

- The Internet Crime Report for 2021, released by USA's Internet Crime Complaint Centre (IC3) of the FBI, has revealed that India stands third in the world among the top 20 countries that are victims of Internet crimes.
- An organisation in India faced an average of 2,807 attacks per week in Q1 2024, a 33% year-on-year increase, making it one of the most targeted nations worldwide.

The **implications** on security of India due to cyber-attacks can be seen from the following examples:

- In 2012, a high profile cyber-attack breached the email accounts of about 12,000 people, including those of officials from the Ministry of External Affairs, Ministry of Home Affairs, Defence Research and



Development Organisation (DRDO), and the Indo-Tibetan Border Police (ITBP).

- In 2013, The Executive Director of the Nuclear Power Corporation of India (NPCIL) stated that his company alone was forced to block up to ten targeted attacks a day.
- 32 lakh debit cards were compromised in 2016.
- Hacking of emails and twitter accounts by a group of hackers who call themselves 'Legion'. This group also claimed access to "over 40,000 servers" in India, "encryption keys and certificates" used by some Indian banks, and confidential medical data housed in "servers of private hospital chains".
- The food tech company Zomato discovered that data, including names, email IDs and hashed passwords, of 17 million users was stolen by an 'ethical' hacker- who demanded the company must acknowledge its security vulnerabilities- and put up for sale on the dark web.
- The global WannaCry ransomware attack took its toll n India with several thousands computers getting locked down by ransom seeking hackers. The attack also impacted systems belonging to Andhra Pradesh police and state utilities of West Bengal.
- The Petya Ransomware attack in 2017 impacted the container handling functions at a terminal operated by Danish firm at Mumbai's Jawaharlal Nehru Port Trust.

2.2. Steps taken by Government in Cybersecurity

Government has taken a number of steps to acquire and increase capacity in the field of cybersecurity. They fall under the Legal framework, Institutional framework and Other measures mentioned in following sections 2.3, 2.4 and 2.5 respectively.

2.3. Legal Framework

2.3.1. National Cybersecurity Strategy 2020

Conceptualised by the Data Security Council of India (DSCI), headed by Lt General Rajesh Pant, it focuses on 21 areas to ensure a safe, secure, trusted, resilient, and vibrant cyberspace for India. The main sectors of focus of the report are:-

- **Large scale digitisation of public services:** Focus on security in the early stages of design in all digitisation initiatives, developing institutional capability for assessment, evaluation, certification, and rating of the core devices and timely reporting of vulnerabilities and incidents.
- **Supply chain security:** Monitoring and mapping of the supply chain of the Integrated circuits (ICT) and electronics products, scaling up product testing and certification, leverage the country's semiconductor design capabilities globally at strategic, tactical and technical level.
- **Critical information infrastructure protection:** Integrating Supervisory control and data acquisition (SCADA) security with enterprise security, monitoring digitisation of devices, evaluating security devices, maintaining a repository of vulnerabilities, preparing an aggregate level security baseline of the sector and tracking its controls, devising audit parameters for threat preparedness and developing cyber-insurance products.
- **Digital payments:** Mapping and modelling of devices and platform deployed, supply chain, transacting entities, payment flows, interfaces and data exchange, routine threat modelling exercises to disclose vulnerabilities, threat research and sharing of threat intelligence, timely disclosure of vulnerabilities.

- **State-level cyber security:** Developing state-level cybersecurity policies, allocation of dedicated funds, critical scrutiny of digitization plans, guidelines for security architecture, operations, and governance.
- **Security of small and medium businesses:** Policy intervention in cybersecurity granting incentives for higher level of cybersecurity preparedness, developing security standards, frameworks, and architectures for the adoption of Internet of Things (IoT) and industrialisation.

2.3.2. National Cybersecurity Policy 2013

It was brought in the backdrop of **revelations by Edward Snowden** of the massive NSA surveillance program. Its key provisions include-

- Set up a 24×7 National Critical Information Infrastructure Protection Centre (**NCIIPC**) for protecting critical infrastructure of the country
- Create a task force of **5,00,000 cyber security professionals** in next five years.
- Provide fiscal schemes and benefits to businesses for adoption of standard security practices.
- Designate **CERT-In** as the national nodal agency to co-ordinate cyber security related matters and have the local (state) CERT bodies to co-ordinate at the respective levels.
- Use of **Open Standards** for Cyber Security.
- Develop a **dynamic legal framework** to address cyber security challenges
- Encourage wider use of **Public Key Infrastructure (PKI)** for government services.
- Engage information security professionals / organizations to assist e-Governance initiatives, establish Centers of Excellence, cyber security concept labs for awareness and skill development through PPP - a common theme across all initiatives mentioned in this policy.

Key concerns

- The National Cyber Security Policy 2013 **mainly covers defensive and response measures** and makes no mention of the need to develop offensive capacity.
- The cyber security policy suffers from **lack of proper implementation** with respect to provisions like recruitment of 5 lakh professionals etc.
- It is inadequate to balance cybersecurity needs with the need to **protect civil liberties** of Indians including privacy rights.

2.3.3. Information Technology Act 2000

The Information Technology Act, 2000 regulates the use of computer systems and computer networks, and their data. The Act gives **statutory recognition to electronic contracts and deals** with electronic authentication, digital signatures, cybercrimes, liability of network service providers etc.

The act lists down, among other things, following as offences:

- Hacking a computer system

- Act of cyber terrorism i.e. accessing a protected system with the intention of threatening the unity, integrity, sovereignty or security of the country.
- Cheating using computer resources
- Tampering with computer source documents

Criminal Offences	Subsection
Sending offensive messages, including attachments, through communications service	66A
Dishonestly receiving stolen computer resource or communication device	66B
Identity theft	66C
Cheating by personating	66D
Violation of privacy	66E
Cyber terrorism: defined as causing denial of service, illegal access, introducing a virus in any of the **critical information infrastructure** of the country defined u/s 70 with the intent to threaten the unity, integrity, security or sovereignty of India or strike terror in the people or any section of the people; or gaining illegal access to data or database that is restricted for reasons of the security of state or friendly relations with foreign states.	66F
Publishing or transmitting of material containing sexually explicit act in electronic form	67A
Publishing or transmitting of material depicting children in sexually explicit act	67B
Preservation and retention of information by intermediaries as may be specified for such duration and in such manner and format as the central government may prescribe.	67C

Limitations of the IT Act

- The issues relating to **confidential information and data** of corporates and their adequate protection have not been adequately addressed.
- The maximum damage, by way of compensation, stipulated by the cyber law amendments is **Rs.5 crores.** This is a small figure and hardly provides any effective relief to corporates.
- The **issue pertaining to spam** has not been dealt with in a comprehensive manner. In fact, the word 'spam' is not even mentioned anywhere in the IT Amendment Act. It is pertinent to note that the countries like U.S.A., Australia and New Zealand have demonstrated their intentions to fight against spam by coming across with dedicated anti-spam legislations. This make India a haven, as for spams it does not address **jurisdictional issues.** Numerous activities on the internet take place in different jurisdictions and that there is a need for enabling the Indian authorities to assume enabling jurisdiction over data and information impacting India, in a more comprehensive way than in the manner as sketchily provided under the current law.

2.3.4. Draft Information Technology (Intermediary Guidelines (Amendment) Rules) 2018 to deal with cyber crimes

Key Features of the Rules

- The Intermediary Guidelines Rules, 2011 require intermediaries to prohibit users from hosting certain content on its platform (e.g. obscene content). The Draft Rules prohibit a new category of information, i.e., content which threatens 'public health or safety'.
- Intermediaries must, within 72 hours, provide assistance to any government agency. Further, they must enable tracing of the originator of the information on their platform.

Intermediaries are entities that store or transmit data on behalf of other persons, and include internet or telecom service providers, and online market places.

The **Information Technology Act** was amended in 2008 to provide exemption to intermediaries from liability for any third party information, among others. Following this, the IT (Intermediary Guidelines) Rules, 2011 were framed under Section 79(2) of the Act to specify the due diligence requirements for intermediaries to claim such exemption

- Intermediaries must deploy technology-based automated tools to identify and remove public access to unlawful information. Further, intermediaries with more than fifty lakh users must incorporate a company in India.

Key Issues and Analysis

- Intermediaries are required to prohibit publication of content that threatens public health or safety. This may violate the right to free speech under Article 19(1).
- Intermediaries are required to deploy automated tools for removing access to unlawful content. This may be contrary to the reasoning of a recent Supreme Court judgement.
- Intermediaries with more than fifty lakh users must incorporate a company in India. It is unclear as to how this number will be calculated. Therefore, an intermediary will find it difficult to determine if it is required to set up a company in India under this provision

2.3.5. National Digital Communication Policy, 2018

A new NDCP-2018 was unveiled to replace the National Telecom Policy, 2012, to cater to the current needs of the digital communication sector. It aims to attract USD 100 billion worth of investments and generate 4 million jobs in the sector by 2022. The policy envisages 3 missions:

- **Connect India:** For creating a robust digital communications infrastructure.
- **Propel India:** For enabling next generation technologies and services through investments, innovation and IPR generation
- **Secure India:** For ensuring sovereignty, safety and security of digital communications

Recently multiple organizations like RBI, SEBI and CERT-In came out with various guidelines on cyber security, as follows:

RBI's Draft Directions on Cyber Resilience and Master Digital Payment Security Controls for Payment System Operators (PSOS).	CERT-In "Guidelines on Information Security Practices" for government entities	SEBI proposes a consolidated cybersecurity framework for SEBI-Regulated Entities (RES).
Coverage: The draft directions governance cover mechanisms for the identification, assessment, monitoring, and management cybersecurity risks. of **Aim:** To ensure that authorized non-bank PSOs are resilient to traditional and emerging information systems and cyber security risks. **Responsibility:** **The board of the PSOs** will be responsible for ensuring adequate oversight over information security risks.	These guidelines are issued under the powers conferred by **section 70B of the Information Technology Act, 2000.** It applies to all Ministries, Departments, and Offices specified in **the First Schedule to the Government of India (Allocation of Business) Rules, 1961.** **Key guidelines** Report security breaches within **six hours of being noticed** Mandatory **cyber security audits every six months** **Employees to be logged out** when inactive for more than 15 minutes Admin access to the system only with the approval of the **chief information security officer**	It aims at providing a **common structure for multiple approaches** to cyber security to prevent any cyber risks/ incidents. The framework is based on five concurrent and continuous functions of cyber security- Identify, Protect, Detect, Respond, and Recover. It has been defined by the **National Institute of Standards and Technology (NIST).** **These functions serve as the pillars** upon which the framework is built, guiding regulated entities in establishing robust cyber security protocols. All REs shall formulate an up-to-date **Cyber Crisis Management Plan (CCMP).** REs would also have to put in place a **comprehensive incident response management plan** and respective Standard Operating Procedures (SOPs).

2.4. Institutional Framework

2.4.1. National Cybersecurity Coordination Centre (NCCC),

It is India's **cyberspace intelligence agency** under CERT-In which will conduct security and electronic surveillance. It aims to **screen communications metadata** coming into the country to detect **real-time cyber threats** and work in close coordination with various law-enforcement agencies for intelligence gathering. The body, functioning under the IT ministry, would strengthen the country's cybersecurity posture. Some have expressed concern that the body could encroach on citizens' privacy and civil-liberties, given the lack of explicit privacy laws in the country.

2.4.2. India's Computer Emergency Response Team (CERT-In)

The CERT-In has been established to thwart cyber-attacks in India. It is mandated under the IT Amendment Act, 2008 to serve as the **national agency in charge of cyber security.**

- **Charter-** "The purpose of the CERT-In is, to become the nation's most trusted referral agency of the Indian Community for responding to computer security incidents as and when they occur"
- **Mission-** "To enhance the security of India's Communications and Information Infrastructure through proactive action and effective collaboration."
- **Constituency -** The CERT-In's constituency is the Indian Cyber-community.

CERT-Fin has also been established based as a specialized agency on the recommendation of a sub-committee of the Financial Stability and Development Council **(FSDC)** to tackle threats related to the financial sector.

2.4.3. National Critical Information Infrastructure Protection Centre (NCIIPC)

It is designated as the National Nodal Agency in respect of Critical Information Infrastructure Protection. Its Functions and Duties are

- protecting nation's critical information infrastructure
- Identification of all critical information infrastructure elements
- Developing and executing national and international cooperation strategies for protection of Critical Information Infrastructure.

All organisations providing digital services have been mandated to report cyber security incidents to CERT-In expeditiously. CERT-In, in turn, issue alerts and advisories regarding cyber threats and counter-measures to all the stakeholders.

About Critical Information Infrastructure

- It refers to those **essential physical and information technology facilities,** which, if disrupted or destroyed, would impact health, safety, security, economic or social well-being of the nation.
  - Dams, Power and Energy, Banking and Financial services, government facilities, healthcare, IT, transportation, nuclear reactors etc are considered parts of the Critical Infrastructure of a country.
- CII is **declared by government under Section 70 of Information Technology (IT) Act, 2000** (amended in 2008).
  - Recently, Census and National Population Register(NPR) database, ICICI and HDFC banks and NPCI's IT resources were declared as Critical Infrastructure by the government.

2.4.4. Indian Cyber-Crime Coordination Centre (I4C) and Cyber Warrior Police Force

These have been established under newly created **Cyber and Information Security (CIS) Division** (under Ministry of Home Affairs) to tackle internet crimes such as cyber threats, child pornography and online stalking.

- **Indian Cyber Crime Coordination Centre** (I4C) has been designated as the nodal agency in the fight against cybercrime.
- Also recently, India created a **National Counter Ransomware Taskforce,** on the lines of the International Counter Ransomware Taskforce, with representation from the finance and legal affairs departments, under the MHA.

2.4.5. Cyber Swachchta Kendra (CSK)

Minister of Electronics and Information Technology launched the Cyber Swachchta Kendra–**Botnet Cleaning and Malware Analysis Centre** for analysis of malware and botnets that affect networks and systems. It is part of Digital India initiative. This centre will work in coordination with the internet service providers (ISPs) and Industry and will also enhance awareness among citizens regarding botnet and malware infection.

CSK provides **various tools** to prevent cyberattacks, like-

- **M Kavach:** Special anti-virus tool for smartphones and tablets.
- **USB Pratirodh:** It is a USB protector to help clean various external storage devices like USB(s), memory cards, external hard disks, etc.
- **AppSamvid:** This is a whitelisting tool for the desktop.
- **Browser JSGuard:** It helps to block malicious JavaScript and HTML files while browsing the web.
- **Free Bot Removal Tool:** It's a QuickHeal partner tool.

2.5. Other Measures

2.5.1. Digital Army Programme

A dedicated cloud to digitize and automate processes, procedures and services for the Indian Army, launched as a part of Digital India. This is similar to Meghraj, the national cloud initiative.

State Government Initiatives to deal with Cyber crime

Telangana: The first state to come up with a policy on cybersecurity. Recently, it established a **Cybersecurity Center of Excellence (CCoE),** in a joint initiative with Data Security Council of India (DSCI).

Kerala: Cyberdome is a Center of Excellence for Kerala Police, to meet the long term security challenges in the digital arena, of the modern world, by bridging the gap between the latest changes and innovations in the cyberspace and the skill set development of Kerala Police , in combating the emerging cyber threats.

Maharashtra- Launched a **'Cyber Safe Women' initiative** under which awareness camps will be held across all the districts of the state regarding cyber safety.

2.5.2. Cooperation with other countries

India along with other countries is undertaking mutual sharing of information and best-practices, both of which are critical in constructing a robust response to conspicuous cyber incidents. For instance, India is working with UK, USA, China, Malaysia, Singapore, Japan and many other countries on diverse issues such as joint training of cybersecurity professionals, information exchange, law enforcement and technical capacity building to jointly combat cybercriminal activity.

2.5.3. Audit of government websites and applications

Empanelment of security auditing organisations to support and audit implementation of Information security best practices

2.5.4. Formulation of Crisis Management Plan for countering cyber attacks

Conducting cyber security mock drills and exercises regularly to enable assessment of cyber security posture and preparedness of organizations in Government and critical sectors.

Conducting regular training programmes for network / system administrators and Chief Information Security Officers (CISOs) of Government and critical sector organisations regarding securing the IT infrastructure and mitigating cyber attacks.

2.5.5. TechSagar Platform

The National Cyber Security Coordinator's office in partnership with the Data Security Council of India launched the online portal which provides actionable insights about the capabilities of the Indian Industry, academia and research across various technology areas including Internet of Things (IOT), Artificial Intelligence (AI), etc. It will facilitate new opportunities for businesses and academia to collaborate, connect and innovate in the future.

2.5.6. Training of Information Security Personnel

Training of 1.14 lakh persons through 52 institutions under the Information Security Education and Awareness Project (ISEA)- a project to raise awareness and to provide research, education and training in the field of information security.

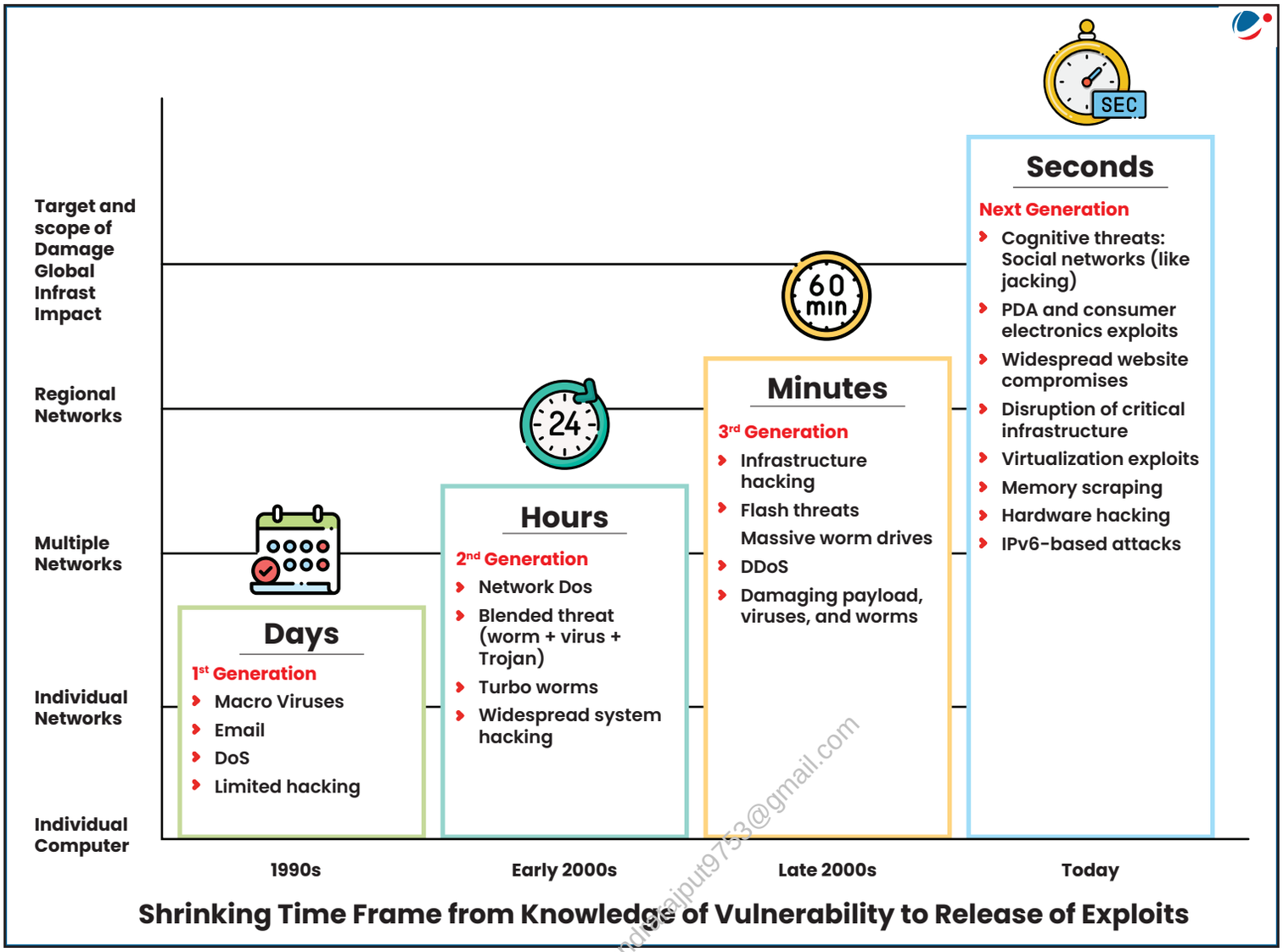
2.5.7. Bharat NCX

- National Cyber Security Incident Response Exercise (Bharat NCX or NCX India) aims to train senior management and technical personnel of Government/Critical Sector organisations on contemporary cyber threats and handling cyber incidents and response.
- NCX India will help strategic leaders to better understand cyber threats, assess readiness, and develop skills for cyber crisis management and cooperation.
- It is being conducted by the National Security Council Secretariat (NSCS) since 2022.

2.6. Challenges to Cybersecurity in India

2.6.1. Structural

- The rapid rate of growth of this sector in both scope and meaning of cybersecurity.
- Internet, by its design, has been created for openness and connectivity and not for ensuring security and protection from unauthorized access.
- There is an ever increasing lag in the pace of proliferation of technology and the development of security architecture around them.



Shrinking Time Frame from Knowledge of Vulnerability to Release of Exploits

2.6.2. Administrative

- Lack of best practices and statutory backing for the same, e.g.- The norms for disclosure of cyber attacks were only put in place in 2019, 6 years after the policy came into being.
- Security audit does not occur periodically, nor does it adhere to the international standards.
- The government is yet to identify and implement measures to protect "critical information infrastructure".
- The appointment of National Cyber Security Coordinator in 2014 has not been supplemented by the creating liaison officers in states.

2.6.3. Human Resource Related

- Huge **under-staffing** of CERT-In.
- **Attitudinal apathy** of users towards issues of cybersecurity.
- Inadequate research in academia.

2.6.4. Procedural

- Lack of **awareness** in local police of various provisions of IT Act, 2000 and also of IPC related to cybercrimes.
- Post-demonetisation, there has been a push to go 'cashless', without building capacity and awareness on the security of devices or transactions thus increasing vulnerability.
- Also, the core infrastructure elements of a smart city cover urban mobility, water and electricity supply, sanitation, housing, e-governance, health and education, security and sustainability, all bounded and harnessed by the power of information technology (IT). Given the massive use of IT in the delivery and management of core infrastructure services, the volume of citizen data generated in a smart city is expected to grow exponentially over time. The current IT Act might not give adequate protection to the citizen data that smart cities will generate.

2.7. Global Cyber Strategy

The United Nations General Assembly has regularly passed resolutions on information security. Several regional initiatives like the European Convention on Cybercrime have been in existence for decades. These efforts can be consolidated in the form of a global cyberspace convention.

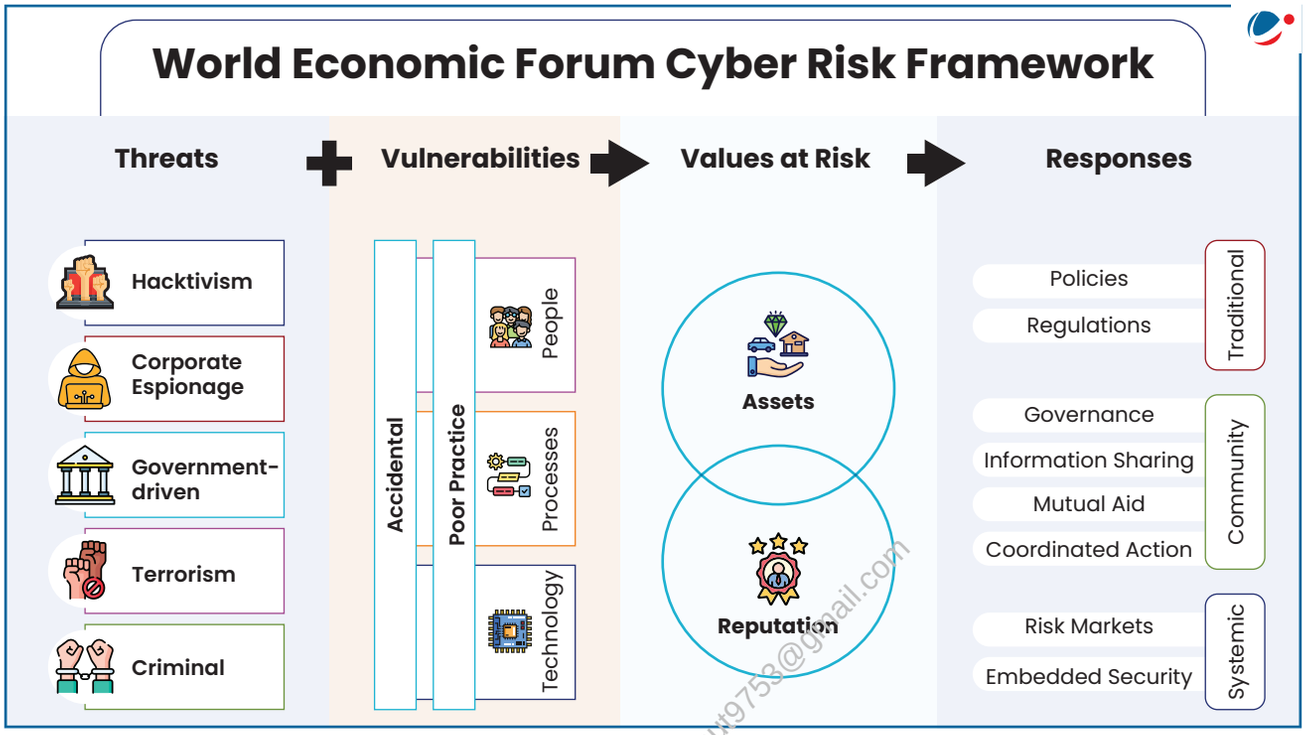
2.7.1. Need of a global strategy

- Risks in cyberspace can destabilize international and national security.
- The growth of social media (Twitter, Facebook, etc.) has created a new medium for strategic communication that by-passes national boundaries and national authorities.
- The global data transmission infrastructure also depends critically on the network of undersea cables, which is highly vulnerable to accidents and motivated disruptions.

2.7.2. Key Components of such Global Cyber Strategy

- National critical infrastructures should not be harmed.
- Secure, stable and reliable functioning of the Internet should be ensured.
- A common understanding of Internet security issues should be evolved.
- National governments should have the sovereign right to make national policies on ICT consistent with international norms.
- A global **culture of cyber security** based on trust and security should be encouraged.
- The digital divide should be overcome.
- International cooperation should be strengthened.
- PPP should be encouraged.
- **CIA (Confidentiality – Integrity – Availability)** of information systems should be ensured.
- Balance between the need to maintain law and order and fundamental human rights should be maintained.

- It would put the obligations on states not to take any overt or clandestine measures which would result in cyber warfare.
- It would also define what the use of force in cyberspace means and in what circumstances such force can be used, if at all.
- The options available with the state if it is subjected to cyber attacks by another state, or a non-state actor, or by a combination of the two.



2.7.3. Why should India not join these Global Efforts?

- These may lead to technology control regimes like those existing in other fields like- space, missile etc. undermining national sovereign interests of India.
- Such treaties like the European Convention of Cybercrime are biased in favour of the requirements of the major international players/powers
- India should first develop its own cyber capabilities to a level that they are beyond the ambit of control regimes.

2.7.4. Why should India join these Global Efforts?

- Isolationist approach derives little or no benefits of the opportunities that arise by engaging with these treaties and conventions.
- As these treaties and conventions are in their infancy and undergoing development. India can proactively engage in drafting them, thus, moulding them to suit its sovereign interests.

2.7.5. Global initiatives

Budapest Convention

- It is the only multilateral treaty on cyber security that addresses Internet and computer crime
- Its focus is on harmonizing national laws, improving legal authorities for investigative techniques and increasing cooperation among nations.
- Developing countries including India have not signed it stating that the developed countries lead by the US drafted it without consulting them

Ground Zero Summit

Ground Zero Summit is the largest collaborative platform in Asia for Cyber security experts and researchers to address emerging cyber security challenges and demonstrate cutting-edge technologies. It is the exclusive platform in the region providing opportunities to establish and strengthen relationships between corporate, public sector undertakings (PSUs), government departments, security and defense establishments.

- The Summit gets its name from a piece of ancient Indian history. India is the ground where zero was discovered and zero is an integral part of digital systems.
- It is being organized by the Indian Infosec Consortium (IIC), which is an independent not-for-profit organization formed by leading cyber experts.
- Aim of the summit: The summit was organized to deliberate upon various issues related to cyber security challenges emerging due to the latest technological developments.
- The theme for the Summit - Digital India – 'Securing Digital India'

ICANN

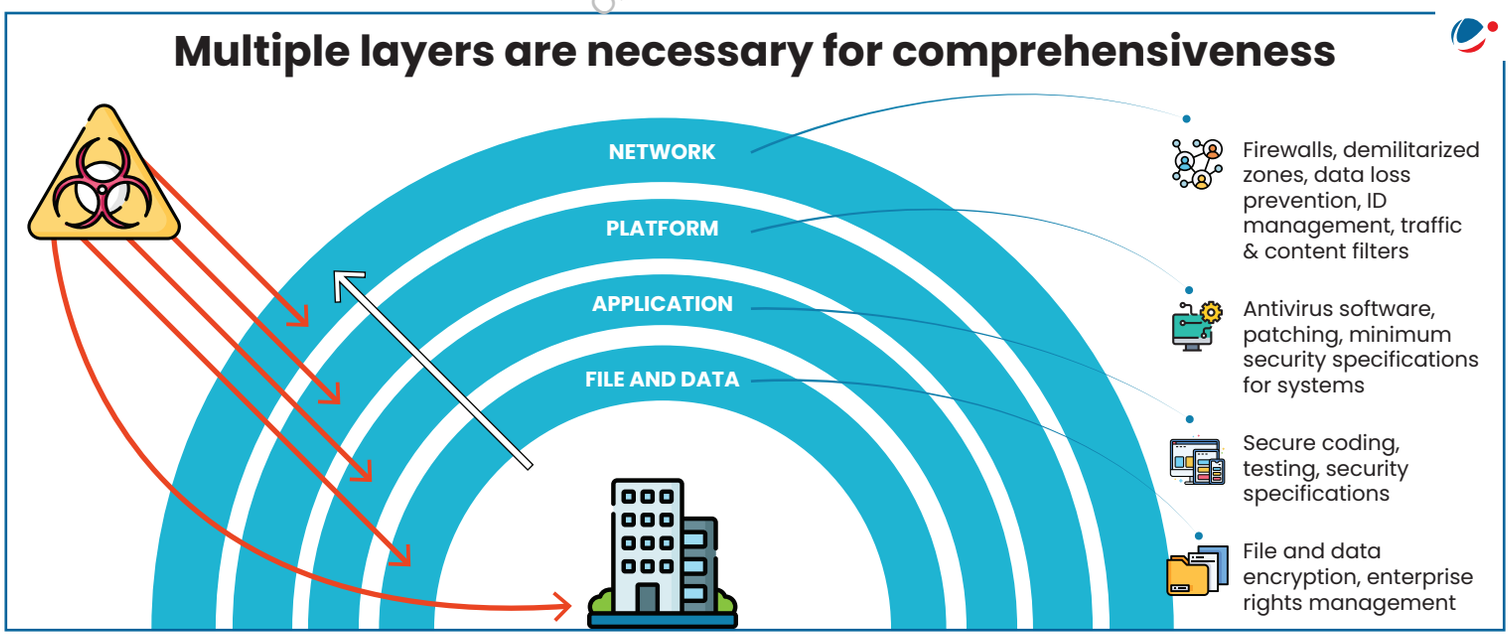
- ICANN, or the Internet Corporation for Assigned Names and Numbers, is a non-profit public benefit corporation and also a global multi-stakeholder organization that was created by the U.S. government.
- It coordinates the Internet Domain Name Servers, IP addresses and autonomous system numbers, which involves a continued management of these evolving systems and the protocols that underlie them.
- While ICANN began in the U.S. government, it is now an international, community-driven organization independent of any one government.
- ICANN collaborates with a variety of stakeholders including companies, individuals, and governments to ensure the continued success of the Internet. It holds meetings three times a year, switching the international location for each meeting.

2.8. Way forward

Cyber warfare encompasses public and private domains. There is a requirement for intimate involvement of the private sector, as they are equal, if not larger, stakeholders. Regular meetings must be held and, if needed, working groups created. Current organisations which could be tasked to take on the cyber warfare challenge include the NTRO, DRDO, RAW and IB, representatives of CERT, NASSCOM, etc. Various measures which may be taken by government of India are as follows:

- India can raise a **cyber command** with responsibility of combating cyberwarfare should be of the Armed Forces along with the DRDO and other experts.

- **Perception management and social networks** should be handled carefully as the "instant availability of information" provides a potential tool for psychological and no-contact warfare. It should form part of any offensive or defensive action.
- Adequate **capacity building** should be done with required investment and R&D as apart from being critical from a security point of view, this field is going to create millions of jobs in the future which India can benefit from.
- **Legal aspects** of developing capacities, understanding use of cyberspace as a "force", implications of the UN Charter, negotiating international laws and treaties – all of this needs trained personnel. All this needs special attention.
- **PPP Model for Cybersecurity:** As the private sector is an equally important partner in providing critical information infrastructure (e.g.- telecom sector which is mostly governed by private players), there is a need to work with the private sector using **Public-Private Partnership** model.
- A mechanism for **information sharing and coordination** between government sector like CERT-In and private sector through Security Information Sharing and Analysis Centres should be established.
- **Education in cyberspace:** Emerging challenges in cybersecurity will need a **bright future in education** in the subject domain. There is a need for resources to assist the academic staff and graduates to understand the needed skills and opportunities. Courses on Computer Science, Information Technology, Systems Design, etc can be offered over National Knowledge Network in MOOC model.
- Assurance Framework: Framework of assurance shall be established to provide guidance on security certifications, qualification criteria and prescribe security audits of gov. ICT systems, Projects & applications
- The government can put in place a **regulatory mechanism** to ensure protection of private sector Critical Information Infrastructure and should also provide incentives for adhering to such norms.
- Indian government along with NASSCOM should **promote startups** working in the field of digital security.
- India can follow **international best practices** such as Tallinn Manual which is an academic work related to laws that apply to cyber-crimes which developed nations such as the USA are following.
- Need for a layered defence for a comprehensive cyber security framework



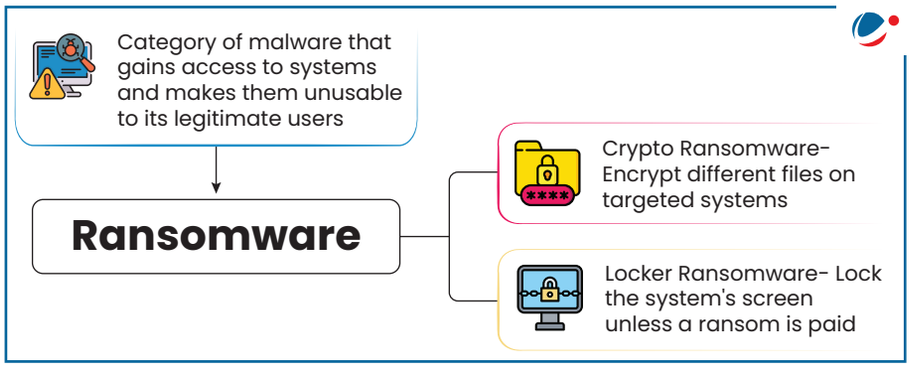
3. Miscellaneous

3.1. Ransomware Cyber Attacks

In 2017, a ransomware called Wannacry, infected more than 100,000 computers all over the world. There are many types of malware that affect a computer, ranging from those that steal information to those that just delete everything on the device. The country most affected by WannaCry was UK, where National Health Service trusts were impacted, causing widespread disruption to health services.

Effect on India

- India's vulnerability was higher because most official computers run Windows and regular updates were not a habit.
- A lot of personal data online is now connected to the Aadhaar data and therefore future such attacks can make privacy of millions of Indians vulnerable.



Another ransomware attack named **Petya** was reported about which CERT-In issued an advisory.

Ransomware Report-2022 released by Indian Computer Emergency Response Team (CERT-In).

Key highlights of the report

- Ransomware incidents have gone up by 53% in 2022 over 2021.
- Not only money, but Geo political conflicts also influenced ransomware attacks this year.
- Broadened Ransomware attacks across critical sectors with increased frequency and complexity.
  - IT and IT-enabled services sector was the most impacted sector, followed by finance and manufacturing sectors.
    - » The servers of the AIIMS are hacked for the seventh day in a row after a ransomware attack.
- Lockbit was the most prevalent ransomware variant in India, followed by Makop and DJVU/Stop ransomware. New variants such as Vice Society and BlueSky were noticed in 2022.
  - Makop and Phobos Ransomware families mainly targeted medium and small organizations, while Djvu/Stop variants used for attacks on individuals.
- Ransomware-as-a-service (RaaS) ecosystem becoming prominent

3.2. Issue of Encryption in India

Under **Section 84A** of Information Technology Act, 2000 Rules are to be framed to prescribe modes or methods for encryption. In this regard, a draft National Encryption Policy was formulated by an Expert Group setup by the Government. However, the draft policy was withdrawn later. The aim was to enable information security environment and secure transactions in Cyber Space for individuals, businesses, Government including nationally critical information systems and networks.

Key features of the policy included:

- Storing the plain text of the encrypted messages for **90 days** by all citizens and provide it to law enforcement agencies as and when required.
- All vendors of encryption products need to **register their products** with the designated agency of the Government
- All encryption technology used in India shall be cleared by the government and only those encryption technologies can be used which are in the government's **prescribed list.** It means government knows every encryption technology used in India

Key concerns

- Policy affected almost all Internet users- a majority of them were **not even aware** that they were using encryption technologies.
- **"On demand"** need to store all communication in plain text for 90 days and making it available to law enforcement agencies poses challenges like - Most of the users in India do not know the meaning of plain text and in such a case they can be held liable for not storing their encrypted data in plain text format.
- Additionally, service providers located within and outside India, using encryption technology for providing any type of services in India, would be required to enter into an agreement with the government. This is 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.
- Keeping a **copy of the data** will require huge storage and that will come at a cost.
- There is a fear that the policy will start a **new "registration raj",** now that all encryption technologies that can be used in India will need to be certified and listed by the agencies concerned.

However, India needs encryption policy due to following reasons:

- To promote use of encryption for ensuring the **security/confidentiality** of internet communication and transactions
- To **facilitate investigation** of crimes and threats to national security in the age of sophisticated encryption technology
- To promote **research** in encryption technology as it is restricted and not available to India under Wassenaar agreement.
- To **build consumer confidence** in retail and e-governance, encouraging more Indians to go online and strengthening the country's underdeveloped cybersecurity sector.
- To check **misuse** of encryption.

For example - Take the case of terrorist Abu Dujana's iPhone 7. While dealing with secure devices, law enforcement agencies themselves rue the increasing use of encryption. Thus far, Indian intelligence agencies have relied on **'zero days' — vulnerabilities** that exist in the original design of a software — to break into encrypted devices, but Internet companies now promptly patch their flaws, diminishing the utility of such tools.

The reality is that a lot of online content is today out of the reach of law enforcement officials. Platforms like WhatsApp and Telegram are **'end-to-end' encrypted,** making it difficult for police at the State and local level — who don't have access to zero days — to register cases based on information contained in them. The distinct trend towards greater adoption of encryption poses a dilemma for Indian policymakers.

Strong encryption protocols increase consumer confidence in the digital economy, but the Indian government fears a scenario where criminals or terrorists can easily "go dark" behind secure channels.

Way ahead for new policy

The policy should leave **room for innovation** in the field of encryption technology so that industry leaders have incentives to innovate and offer consumers more secure information services. The policy should go for securing information through a minimum standard, instead of rendering it insecure by dictating a standard that might get obsolete.

The policy must be sensitive to the need to promote cybersecurity research in India. The **process to retrieve encrypted data** must be transparent and necessarily be backed by a court warrant from a civil court, obtained through an open judicial hearing. The policy should provide guidance on the use of information/ data within the country in a regulated manner and ensure that our government agencies can access them for investigating serious issues related to terrorism, national security and critical infrastructure.

The new policy would need to focus on enterprises such as e-commerce companies to ensure their encryption were good enough to secure customer's financial and personal data. The policy should prescribe technologies which are globally accepted. It should also talk about revising them from time to time, which is very important as this is a dynamic space.

3.3 Digital Personal Data Protection Act, 2023

3.3.1. Background

- In 2017, the Supreme Court recognised privacy as a fundamental right in the K.S. Puttaswamy vs. Union of India case.
- Following this, the Justice Srikrishna Committee (established by the Ministry of Electronics and Information Technology (MeitY)) proposed the initial draft of the Personal Data Protection (PDP) Bill in 2018.
- The government revised the draft and introduced it as the PDP Bill 2019.
- However, in 2022, the government withdrew the PDP Bill 2019 by citing the extensive changes made by the Joint Committee of Parliament to it.
- MeitY released a draft of the DPDP Bill 2022 for public consultations, which later became the DPDP Act 2023.

3.3.2. Key features of the Act

- It protects digital personal data (that is, the data by which a person may be identified) by providing:
  - The obligations of **Data Fiduciaries** (that is, persons, companies and government entities who process data) for data processing (that is, collection, storage or any other operation on personal data);
  - The rights and duties of **Data Principals** (that is, the person to whom the data relates);
  - **Financial penalties** for breach of rights, duties, and obligations.
- Provides for the establishment of **Data Protection Board of India (DPBI)** by the Central government for
  - Monitoring compliance and imposing penalties.

- Directing data fiduciaries to take necessary measures in event of a data breach.
- Hearing grievances made by affected persons.

- Bill **allows the transfer of personal data outside India,** except to countries restricted by the government.
- The **central government may exempt certain activities** in the interest of the security and public order.
- The Act provides that the data fiduciary will not undertake any processing that has a detrimental effect on the **well-being of a child.**

Seven Principles of DPDP Act

- The principle of consented, lawful and transparent use of personal data
- The principle of purpose limitation (use of personal data only for the purpose specified at the time of obtaining the consent of the Data Principal)
- The principle of data minimisation (collection of only as much personal data as is necessary to serve the specified purpose)
- The principle of data accuracy (ensuring data is correct and updated)
- The principle of storage limitation (storing data only till it is needed for the specified purpose)
- The principle of reasonable security safeguards
- The principle of accountability (through adjudication of data breaches and breaches of the provisions of the Act and imposition of penalties for the breaches

3.3.3. Limitations of the Act

- **Violate Fundamental Rights:** Exemptions for the State may lead to data collection, processing, and retention beyond what is necessary and may violate the fundamental right to privacy.
- **Inadequate Safeguard:** The transfer of personal data outside India may not ensure adequate data protection standards in the countries where the transfer of personal data is allowed.
- **No compensation:** The Act has removed Section 43A of the Information Technology (IT) Act, 2000, which mandated companies to compensate users in case of mishandling their data.
- **Complicated approach to grievance redressal:** Aggrieved individuals are required to first approach the data fiduciary's redressal mechanism.
  - Unresolved grievances can be escalated to the Data Protection Board, with further appeals to the TDSAT.
- **RTI Exemption:** The Act proposes that the personal information of public officials will not be disclosed under the Right to Information (RTI) Act, which could aid corrupt practices by not disclosing assets, liabilities etc.
- **Clear definition: T**he Act provides that the data fiduciary will not undertake any processing that has a detrimental effect on the well-being of a child. However, there is no definition of detrimental effect or any guidance for determining such effect.

3.4. Edge Computing

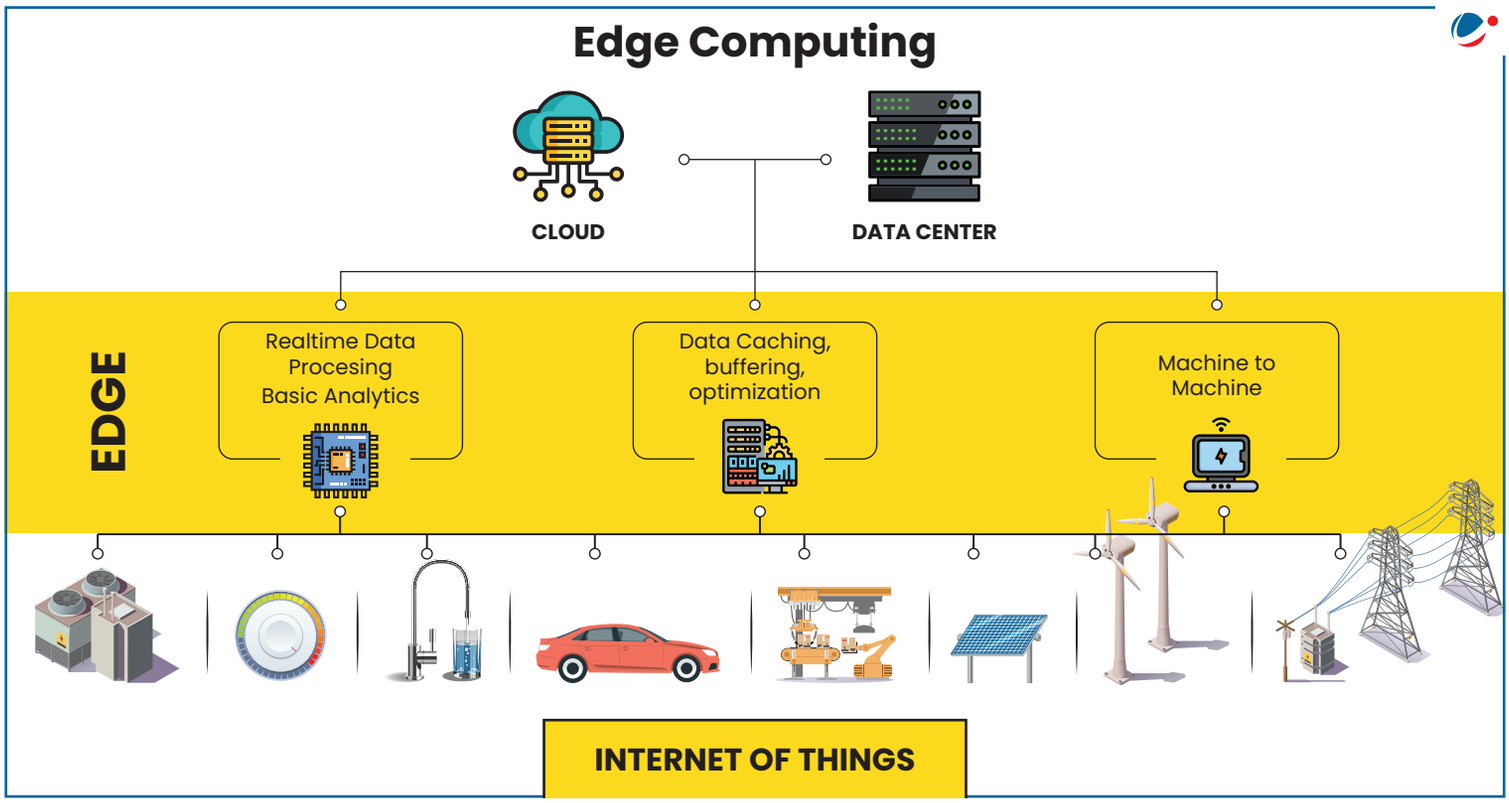
Edge computing enables data to be analysed, processed, and transferred at the edge of a network. Meaning, the data is analysed locally, closer to where it is stored, in real-time without latency.

3.4.1. Benefits of Edge Computing

- **Speed:** The most important benefit of edge computing is its ability to increase network performance by reducing latency (ability to process very high volumes of data with minimal delay). It allows for quicker data processing and content delivery.
- **Security:** Centralized cloud computing architecture is vulnerable to distributed denial of service (DDoS) attacks and power outages.
  - Edge computing distributes processing, storage, and applications across a wide range of devices and data centers, which makes it difficult for any single disruption to take down the network.
  - Since more data is being processed on local devices rather than transmitting it back to a central data center, edge computing also reduces the amount of data actually at risk at any one time.
- **Scalability:**
  - Expanding data collection and analysis no longer requires companies to establish centralized, private data centers, which can be expensive to build, maintain, and replace when it's time to grow again.
  - Edge computing offers a far less expensive route to scalability, allowing companies to expand their computing capacity through a combination of IoT devices and edge data centers.
  - Versatility: The scalability of edge computing also makes it incredibly versatile. By partnering with local edge data centers, companies can easily target desirable markets without having to invest in expensive infrastructure expansion.
- **Reliability:** With IoT edge computing devices and edge data centers positioned closer to end users, there is less chance of a network problem in a distant location affecting local customers. This increases reliability.

How it differs with Cloud Computing?

- The basic difference between edge computing and cloud computing lies in **where the data processing takes place.**
- Cloud computing means storing and accessing data and programs over the Internet instead of your computer's hard drive. Edge computing, on the other hand, manages the massive amounts of data generated by IoT devices by storing and processing data locally.



4. UPSC Mains Previous Years' Questions

1. What are the different elements of cyber security? Keeping in view the challenges in cyber security, examine the extent to which India has successfully developed a comprehensive National Cyber Security Strategy. (2022)
2. Keeping in view India's internal security, analyse the impact of cross-border cyber attacks. Also discuss defensive measures against these sophisticated attacks. (2021)
3. Discuss different types of cyber crimes and measures required to be taken to fight the menace. (2020)
4. What is CyberDome Project? Explain how it can be useful in controlling internet crimes in India. (2019)
5. 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 protection of personal data in cyber space? (2018)
6. Discuss the potential threats of Cyber attack and the security framework to prevent it. (2017)
7. Discuss the advantage and security implications of cloud hosting of server vis-a-vis in-house machine-based hosting for government businesses. (2015)
8. 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. (2015)
9. What is digital signature? What does its authentication mean? Giver various salient built in features of a digital signature. (2013)
10. Cyber warfare is considered by some defense analysts to be a larger threat than even Al Qaeda or terrorism. What do you understand by Cyber warfare? Outline the cyber threats which India is vulnerable to and bring out the state of the country's preparedness to deal with the same. (2013)

5. Vision IAS Mains Previous Years' Questions

1. Economic vitality and national security of a country depend on a stable, safe and resilient cyberspace. In this context, analyse the need for making India's National Cyber Security Strategy robust and effective. Suggest measures that the government needs to take to tackle the escalating cyber threats and espionage.

Approach:

- Introduce the answer by stating how economic vitality and national security of a country are linked to safe and stable cyberspace.
- Highlight the need for making our cyber security strategy effective.
- Discuss the measures to be taken in this context.
- Conclude accordingly.

Answer:

The significance of cyberspace for nations has grown significantly due to rapid increase in usage in the recent times. Its stability and resilience is **critical for India's economic vitality,** as critical economic infrastructure such as financial services (e-kuber), banks, power, manufacturing, etc. are getting digitised in a swift way. Further, it **holds importance for national security,** as cyberspace offers a new dimension to traditional warfare.

However, cyberspace is vulnerable to a variety of incidents and has become very sophisticated and complex with technological innovations. For instance, the number of cyber security incidents in India has gone up to 1,267,564 in 2022 from 41,378 in 2017 as per recent data produced in the Parliament.

Need for making India's Cyber Security Strategy robust and effective:

- **Growing internet base and digitalisation:** India has one of the largest internet user bases in the world with over 800 million internet users. Further, with the concept of **'work from anywhere'** being the norm, there has been a dramatic shift to cloud computing services and mobile workforce, which have accelerated cyber security risks.
- **Vulnerabilities of humongous data:** The local, state and Central governments maintain a huge amount of confidential data related to the country (geographical, strategic military assets, etc.) and citizens. As government offices are scattered across the country, bringing about a common minimum cyber security posture and hygiene poses a huge challenge.
- **Emergence of Artificial Intelligence (AI):** Emergence of AI poses new threats to cyber security infrastructure. For instance, attackers can use AI-driven tools that constantly change their malware signatures to evade detection.
- **State-sponsored cyber threats:** Increasing cases of cyber espionage, cyber terrorism, and ransomware like that of the recent ransomware attack on AIIMS, data breach of Solar India Industries Limited, etc. indicate the possible involvement of state actors like Pakistan and China.

Measures that the government needs to take to tackle cyber threats are, as follows:

- **Institutional measures:** The draft National Cyber Security Strategy stresses on the need for a legislative framework to address the emerging challenges in the technology space. Further, **cyber forensic capacity building** to investigate dark net activities and crypto currency transactions which abet cybercrimes is required.

- **Enhancing coordination of CERT teams:** A broad framework and standard procedure need to be developed for determining CERTs' response to transnational cyber threats and developing resilient cyber systems.
- **Augmentation of cyber security skills:** Diverse and adequate cyber security experts need to be roped in towards building capacity and expertise in this area. Further, specialised cyber units should be formed at the state level comprising officers who have domain knowledge.
- **Upgradation of technology:** There is a need for advanced security technologies such as **API security solutions, XDRs, cloud security tools,** etc. in order to establish a resilient and robust cyber security infrastructure.
- **Crisis management:** The government should hold cyber security drills which include real-life scenarios with their ramifications. Further, in critical sectors, simulation exercises for cross-border scenarios must be held on an inter-country basis.

Cyber security has become an essential aspect of international affairs that requires adequate focus due to its economic and geopolitical implications. The need of the hour is effective implementation of the draft National Cyber Security Strategy to build a safe, trusted and resilient cyberspace.

2. Highlighting the vulnerability of India's critical infrastructure to cyber attacks, discuss the various steps taken by the government to boost cyber security.

Approach:

- Briefly write about India's critical infrastructure.
- Highlight the vulnerability of India's critical infrastructure to cyber attacks.
- Mention the steps taken by the government to boost cyber security in India.
- Conclude accordingly.

Answer:

Critical infrastructure (CI) refers to those essential physical and information technology facilities, networks, services and assets, which, if disrupted or destroyed, would have a serious impact on the health, safety, security, economic or social well-being or the effective functioning of government and the country.

Critical infrastructure in India remains vulnerable to cyber attacks due to the following factors:

- **Import dependence:** Use of imported electronic devices from cell phones to equipment used in power sector, defence, banking, communication etc. puts India in a vulnerable position to cyber attacks.
- **Poor human resources:** India lacks infrastructure and trained staff to deal with the rising incidents of cybercrime.
- **Lack of inter-agency coordination:** There is a lack of coordination among various agencies working for cyber security. Further, the private sector, despite being a major stakeholder in cyberspace, has not been involved proactively for the security of the same.
- **Poor penetration:** There is a lack of adoption of new technology. For example, banking infrastructure is not robust to cope with rising digital crime, which results in data theft related to credit cards and other online frauds.

  Critical infrastructure is deeply interconnected and complex by design and geographically dispersed. These infrastructures are especially vulnerable to attacks, as dedicated weapons systems or armies

are not required to disable these systems. Any delays or disruptions in the functioning of these systems can have a rippling effect across multiple infrastructures, resulting in political, economic, social or national instability.

In this regard, the government has taken the following steps to boost cyber security:

- **Information Technology Act, 2000:** It provides a legal framework for transactions carried out by means of electronic data interchange and other means of electronic communication.
- **Indian Computer Emergency Response Team (CERT-in):** It has been established to enhance India's Communications and Information Infrastructure security through proactive action and effective collaboration. CERT-fin has also been launched exclusively for the financial sector.
- **National Critical Information Infrastructure Protection Centre (NCIIPC):** The centre aims to battle cyber security threats in strategic areas such as air control, nuclear and space.
- **National Cyber Coordination Centre (NCCC):** It is being set up to scan internet traffic coming into the country and provide real time situational awareness and alert various security agencies.
- **Indian Cyber-Crime Coordination Centre (I4C) and Cyber Warrior Police force** have been established under the Ministry of Home Affairs to tackle internet crimes such as cyber threats, child pornography and online stalking.
- **Controller of Certifying Authorities:** It is established under IT Act to license and regulate the working of Certifying Authorities. The Certifying Authorities (CAs) issue digital signature certificates for electronic authentication of users.
- **Digital Army Programme:** It is a dedicated cloud to digitize and automate processes, procedures and services for the Indian Army, launched as a part of Digital India. It is similar to Meghraj, the national cloud initiative.

Looking at the criticality of securing its critical infrastructure, India needs to develop a credible cyber security framework which will provide capability of cyber deterrence.

3. It has been argued that the success of Digital India is critically dependent on the way we handle our cyber security. Examine.

Approach:

- Briefly discuss the Digital India programme.
- Discuss its vulnerability to cyber-attacks.
- Explain the lacunae in our cyber security apparatus that make Digital India programme vulnerable to security threats and how their redress is critical to its success.

Answer:

In order to transform the entire ecosystem of public services through the use of information technology, Government has launched Digital India programme with the vision to transform India into a digitally empowered society and knowledge economy.

Online Cyberspace touches nearly every part of our daily lives through broadband networks, wireless signals and mobile networks. Digital India will further bring all the government and citizens' data and transactions in cyberspace and will bring transparency, efficiency and citizen participation in the public governance.

However, cyber space is under constant threat because:

- India has little control over hardware used in India as well as the information carried on internet.
- India's infrastructure is susceptible to espionage, which involves intruding into systems to steal information of strategic or commercial value; cybercrime, referring to electronic fraud or other acts of serious criminal consequence; attacks, intended at disrupting services or systems for a temporary period; and war, caused by a large-scale and systematic digital assault on India's critical installations.
- Constant cyber attacks in the Banking sector, Social media accounts and even government websites exemplifies the need of having strong cyber security infrastructure.
- No national security architecture that can assess the nature of cyber threats and respond to them effectively.
- Security risk associated with using Open Source Software.
- Lack of personnel trained in cyber-security, although mandated by National Cyber Security Policy (NCSP).

These vulnerabilities in the cyberspace put the success of Digital India programme at risk, in fact, if cyber-security is not adequate then it can cause more harm than benefits. It can threaten the national security, privacy of citizens, financial security and make poor citizens vulnerable to fraud and cheating. Therefore, cyber-security architecture needs to be strengthened for optimising benefits:

- Developing a comprehensive cyber-security policy with emphasis on protection of scyber infrastructure and data.
- Addressing loopholes of NCSP and implementing it earnestly.
- Establishing National Cyber Security Agency (NCSA) guided by a document outlining India's cyber strategy, much like its nuclear doctrine.
- Training of personnel in cyber-security and harnessing the highly skilled IT workforce. Lessons can be learned from China, which has developed robust cyber security infrastructure.
- India should develop legal architecture to deal with increasingly complex cybercrimes.

Thus, it is important that India streamline its cyber-security apparatus for the success of e-governance initiatives and electronic services provided in the country both by government and private enterprises. It would be prudent to take help of private sector, which has developed a world class IT and ITES industry in the country for this purpose.

4. NATGRID has been touted as an idea, which would help a great deal in combating terrorism emerging out of Indian soil. In this context, examine how NATGRID would strengthen India's security architecture.

Approach:

- Start the answer with providing brief background about the genesis and objective of idea of NATGRID.
- Then show how it would be an important tool in strengthening India's security architecture and fighting terrorism.
- Then also highlight some apprehension about this project.
- Then conclude with a positive note with suggesting safeguard against misuse.

Answer:

Background of NATGRID:

- The idea of setting up Natgrid or National Intelligence Grid came into much **focus after 26/11 Mumbai terrorist attack.** The concept behind this is to merge all databases of individuals into one which could be accessed by various agencies.
- The Natgrid is supposed to network and mesh together **21 sets of databases** to achieve quick, seamless and secure access to desired information for intelligence and enforcement agencies.

Benefits and importance:

- **Coordination and cooperation -** Security agencies point out that although India does have a capable policing wing across all states they remain handicapped for the want of data. Take for instance if a terrorist of Gujarat origin is nabbed in Rajasthan, then the police teams of both states will need to coordinate. In the past we have seen due to lack of coordination and most of the time ego clashes between the police departments of both states information is not shared. With Natgrid, this issue would be solved and the respective departments could access the data base without having to coordinate with each other.
- Natgrid would also help the police and the Intelligence Bureau **keep a tab on persons with suspicious backgrounds.** The police would have access to all his data and any movement by this person would also be tracked with the help of this data base. An operational Natgrid, for instance, could have intercepted **David Coleman Headley,** the Pakistani-American terrorist who played a key role in the 26/11 Mumbai attacks, when he undertook nine trips to India between 2006 and 2009.
- **Timely access to information -** When there is an issue with a particular person, the police would have access to that person at the click of a button. Prior to this, the police of a particular state had to call his colleague in another state and after a lot of bureaucratic procedures, the data was shared. This procedure normally took anything between a week or two, which in turn gave time for the person in question to slip out.

Challenges:

- But the apprehensions related to security of private data and its possible misuse by over-zealous officers are creating fear regarding this new security tool.
- Also there will be need to update the data from local police station, which is not an easy task as our police is not that much e-literate.
- There are also issues regarding the agencies, which can access the database.

Although the need for an integrated database for the purpose of India's security from terrorist attacks cannot be overemphasized but there are some outstanding issues/challenges, which are being considered. After addressing them in their entirety only, India can accrue the maximum benefit from NATGRID.

5. Cyberspace, like outer space, is unbounded and equally accessible to all. In this context, evaluate the merits and demerits of having a body like the United Nations to govern it. Also, comment on the role that India has played so far in reforming internet governance structures.

Approach:

The introduction should reflect clear understanding of the current governance structure. Discuss multilateral approach arguments- democratisation v/s centralisation and multiple governments exercising control. Mention the independent position taken by India regarding multilateral approach with participation of multiple stakeholders.

Answer:

Cyberspace is virtual space of all IT systems linked at data level on a global scale. The basis for cyberspace is the Internet as a universal and publically accessible connection and transport network. Currently, the Internet is governed largely by three non-profit institutions- ICANN (International Commission for Assigned Names and Numbers), IETF (Internet Engineering Task Force) and the Internet Society. ICANN is the body that manages Critical Internet Resources (CIRs), such as Domain Name Servers (DNS). These, along with private companies like Verisign, which own .com and .net domains, are incorporated under Californian laws and all the edits they make are audited and approved by the US Department of Commerce (US-DoC). This political oversight by US gives it unilateral power over control of Internet. As Internet has grown and spread across the globe, many countries question as to why the US should have outsize influence over how internet is run.

Cyberspace governance comprises of both issues – the public policy aspects, i.e. freedom, privacy, access and human rights, as well as technical aspects, i.e. management of CIRs. Even though states have laws regarding the former, their implementation will depend on if the states have access to manage of CIRs. In this regard, various models of management of CIRs or, more specifically, the oversight of ICANN have been put forward by different countries. This process has gained currency due to abuse of position by the US as exposed by Edward Snowden.

Countries like Russia and China, which exercise large degree of control over their domestic internet access, have proposed multilateral oversight through International Telecommunications Union (ITU) of the United Nations.

Merits:

- Democratisation of oversight mechanism, with representations of various governments.
- Making nation-States capable to exercise their sovereign right, as per Geneva declaration, to formulate internet public policy with the power to enforce it.
- Curtailing the power of non-state actors to make public policy decisions via technical governance.
- Making use of International Law to extract accountability from ICANN, rather than US specific laws which it is subject to currently.

Demerits:

- Erosion of bottom-up processes- states represent their interest as States (like security and defence) and not as interest of their Citizens. Geo political meddling in a multipolar world will lead to fragmentation of internet.
- Inter-governmental oversight will slow down the advancement and decision making process. With limited understanding of internet architecture and requirements, and threat of veto powers, the hard work of technical community would be vulnerable to be overturned.
- With ITU dominated by telecom service providers, net-neutrality, if not the growth of internet itself, would be under serious threat.

- The institutions meant to enforce international law are only remotely accessible, slow and ineffective. ICANN under the oversight of various countries will make it even less accountable to grievances of individual users.

It can be seen that demerits for having a multilateral body like the UN far outweigh the merits. Upending the fundamentals of the multilateral model is likely to balkanize the Internet at best and suffocate it at worst.

Role played by India in reforming Internet governance structure:

India has been critical of the unilateral control enjoyed by the United States and has advocated for a democratic, transparent and inclusive arrangement for running the medium. Earlier, the Indian position was for a multilateral approach, but lately, it has changed to a multi stakeholder approach– involving civil society and private organisations, so that national governments are held accountable to other stakeholders and vice-versa. Along with proposing a UN Committee for Internet Related policies (UN-CIRP), another demand has been that traffic originating and terminating in a country should stay within that country, rather than routing through servers located under foreign jurisdictions. Even though it has argued for making current system of IP address allocation by ICANN as 'fair, just and equitable', its (ICANN) relationship with CIRP, absence of clear definitions, composition of governing body and precise role of stakeholders is still shrouded in ambiguity.

6. Explain the need and recently faced challenges of Deep Web.

Approach:

- Use the examples of intelligence agencies' surveillance practices and Silk Road to explain the need and challenges respectively.

Answer:

The Deep Web is the part of the Internet that search engines do not reach. There is a lot of information hidden in the form of websites that standard search engines do not find because those pages do not exist until they are created dynamically through a specific search.

It makes use of an anonymity network called 'Tor' which encrypts the data and then distributes the small packets of data across multiple relays set-ups by users across the world.

There is a certain need of deep web these days. With news of intelligence agencies' surveillance practices, it has become crucial to keep critical and important documents private. It can also be the solution for research of sensitive topics, facilitator for hidden military communication and safe submission of sensitive documents to governments, police etc. The journalist community should make maximum use of the Deep Web because it is safer than any other privacy measure.

But it can raise some major challenges also. Deep Web exists in order to provide services to people and organisations that require anonymity to release information or communicate without fear. This can cause some problems. There is a sense of security below the surface of the Deep Web, an assumption that with a bit of vigilance any online action could be invulnerable the law. The Tor browser lets users access and even host websites anonymously, Bitcoins allow payment, and an ever-more efficient global postage system will even deliver. Recently FBI arrested the alleged administrator of a flourishing anonymous online drug market called 'Silk Road'. Apart from drugs there are many such illegal anonymous businesses such as arms dealing and contract killing that are operational. So before using Deep Web frequently, a good cyber security infrastructure has to be put in place.

7. "Indian cyber laws lack teeth to bite data hackers." Analyze.

Approach:

- Explain that the fertile liberal treatment meted out to cyber criminals, by the IT Act, facilitating the environment where they can tamper with, destroy and delete electronic evidence, is likely to make a mockery of the process of law and would put the law enforcement agencies under extreme pressure.

Answer:

The current cyber laws are not sufficient to deal with data hacking in India. A lot more needs to be done under the Indian cyber security law to deal with hackers:

- Indian information technology (IT) laws are not stringent enough to deal with hacking instances. In case any university or institute network is hacked by someone, the maximum punishment is three years and Rs. 5 lakh fine under Section 66 of the Information Technology Act.
- In the 14-odd years since Internet has been commercially introduced in our country, India has got only three cyber crime convictions.
- Hacking is a bailable offence in India, unlike say, the US, where it is a non-bailable offence.
- Keeping in account human behavior and psychology, it will be but natural to expect that the concerned cyber criminal, once released on bail, will immediately go and evaporate, destroy or delete all electronic traces and trails of his having committed any cyber crime, thus making the job of law enforcement agencies to have cyber crime convictions, a near impossibility.
- It is often difficult to attribute guilt using the existing statutes since the act of trespassing into a system and tampering with virtual data is not specifically defined in law.
- In the US and Europe, there is a complete legislation dedicated to data protection. However, under the Indian law, there are only two related provisions. And even under these, there is no clarity.
- While hacking attacks remain under the jurisdiction of cyber laws, it is the lack of privacy laws in India that allows cyber criminals to misuse user's data on social networks.
- Cyber criminals recognize the confusion over cyber laws and are making the most of it. In most forms of cyber attacks on social networks, it is the user who clicks on malicious links and, unknowingly, passes on the virus or spam to his contacts. There are no specific provisions in Indian cyber law to deal with these kinds of threats.
- In the US, when the Sony Playstation network was hacked, users filed lawsuits against the company. In India, users who lost their data could do nothing against the company.
- Cyber crimes like data hacking in India are investigated by a low-level police inspector. The efficacy of such an approach is hardly likely to withstand the test of time, given the current non- exposure and lack of training of Inspector level police officers to cyber crimes, their detection, investigation and prosecution.

The expectations of the nation for effectively tackling cyber crime and stringently punishing cyber criminals have all being let down by the extremely liberal IT act, given their soft corner and indulgence for cyber criminals. All in all, given the glaring loopholes as detailed above, the IT Act are likely to adversely impact all users of computers, computer systems and computer networks, as also data and information in the electronic form.

8. Crisis Management Plan for Cyber Attacks is inadequate without Public Private Partnership (PPP) in Critical Information Infrastructure. Examine.

Approach:

- Role of private players in Critical Information Infrastructure
- Why its security cannot be left alone in private hands alone

Answer:

Department of IT of govt. of India has identified critical IT-dependent infrastructure, namely Defence, Finance, Energy, Transportation and Telecommunications. The following analysis of some of these sectors shows that a significant part of the **Critical Information Infrastructure (CII)** is owned and operated by the private sector in India:

- The telecom sector is mostly governed by private players, except MTNL and BSNL. The global undersea cable communication infrastructure(GUCCI) is largely owned by private players.
- **The banking sector,** where more than30% of the transactions are done online, and the value of these transactions is over 80% of total transaction value, has a large number of foreign and private banks.
- **Stock Exchanges –** The major stock exchanges BSE and NSE are private players, wherein most of the transactions are done through the electronic medium.
- The airline industry is dominated by private players, with Air India being the only government enterprise.
- **Energy and Utilities –** Though this sector is largely dominated by government players, the distribution in major cities is largely controlled by private partners.

Thus, the private sector is equally important when it comes to securing a nation's cyberspace. However, the government cannot leave it to the private sector alone for securing its own CII. This is because if any cyber-attack takes place on CII owned by a private company, the consequences of such an attack may have an adverse impact on the entire nation and not restricted to the company owning the CII. For example, if there is a cyber-attack on one of our national stock exchanges, it could possibly bring down the entire trade operations, impacting the economy and creating panic among investors.

Therefore, there is an urgent need of appropriate collaboration and partnership between the government and the private sector for securing CII and the private sector needs to be greatly involved in government's cyber security initiatives through various mechanisms, which can include PPP in the following areas:

- Security Information Sharing and Analysis
- Innovation in Regulatory Approach
- Innovation in Security Programs
- Pro-active threat and vulnerability management
- Promoting best practices in CII
- Assessing and monitoring security preparedness
- IT supply chain
- Taking leadership and partnership in international efforts like Financial Action Task Force (FATF).
- R&D, capacity building, creating awareness in general masses and collaboration in specific areas such as defence etc. are other prominent areas which seek the PPP in CII.

9. Cyber terrorism holds serious potential to paralyze economic and financial institutions in India. What are the issues and challenges w.r.t. India's cyber security? What initiatives has the GoI taken to address the same?

Approach:

- In the introduction, briefly explain the given statement Identify and delineate the issues and challenges in India's cyber security.
- Mention the measures that have been taken.
- One can also suggest other measures that must be taken to counter such attacks.

Answer:

Cyber terrorism is the convergence of terrorism and cyber space. It is unlawful attacks and threats of attacks against computers, networks, and information stored therein to intimidate or coerce a government or its people in furtherance of political or social objectives.

Issue

This possibility of cyber-terrorism becomes very prominent because of proliferation of IT infrastructure and services across sectors in the economy. For example:

- **Banking:** Most of the Indian banks have gone through computerization and therefore are prone to cyber attacks. For example, recent cyber attack, in late 2016, resulted in loss of bank data of millions of account holders.
- **Finance:** With the push to e-governance program most of the services have already been migrated to digital platform. For e-banking, e-commerce, etc.
- **Economic institutions engaged in the distribution of goods and services** rely heavily on ICT.
- **Critical infrastructure** such as power system, transportation system, refineries are vulnerable to data theft, cyber-attack that could bring whole economy stand still.

Challenges

Cyber security in India faces serious challenges:

- **Digital infrastructure:** In India most people use cheaper smart phones with poor cyber security and privacy features, which makes them prone to cyber attack. For example, in India only 1% people use i-phones, as compared to 44% in USA.
- Lack of awareness and transparency: Lack of awareness and the culture of cyber security at individual as well as institutional level. Moreover, agencies are not willing to declare cyber attacks on their infrastructure.
- **Lack of trained manpower** to counter and investigate cyber attacks.
- **Lack of coordination:** There are many counter cyber attack agencies without effective coordination and information sharing.
- **Data storage elsewhere:** India is net information exporter. Its information highways point west, carrying with them the data of millions of Indians.

Measures already taken

To counter above challenges, following measures have been taken:

- **Dedicated IT infrastructure:** National Informatics Center (NIC) provides the critical network backbone

at various levels of government.

- **CERT-In:** It is very critical agency to detect and counter cyber attacks on real time basis, responsible for pro-active and reactive measures. CERT-In also provides necessary expertise to audit IT infrastructure of critical and other ICT sectors.
- **Cyber Security Policy 2013:** It provided for the creation of dedicated institutions and human resources for countering cyber attacks.
- **I4C (Indian Cyber Crime Coordination Center):** It has been set up in 2016 to look into every kind of cybercrime.
- Government has setup **National Critical Information Infrastructure Protection Centre (NCIIPC)** to protect the critical information infrastructure in the country.
- All the Ministries/ Departments of Central Government and State Governments have been asked to implement the **Crisis Management Plan (CMP)** to counter cyber-attacks and cyber terrorism.
- **Cyber Security mock drills** are regularly conducted to prepare the organizations to detect, mitigate and prevent cyber incidence.
- India has been recognized as **Certificate Issuing Nation** in the area of cyber security under Common Criteria Recognition Arrangement (CCRA).
- Government has initiated **Information Security Education and Awareness (ISEA) project** with the aim to develop human resource in the area of Information Security at various levels
- **Cyber Swachhta Kendra–**Botnet Cleaning and Malware Analysis Centre for analysis of malware and botnets that affect networks and systems.

Though, these measures are important but not sufficient to check the cyber terrorism in India, therefore we need to further build upon these initiatives as under.

Way forward

- **Create awareness:** There is need to sensitize the people and institutions of the need and importance of cyber security measures, to make them report such attacks promptly, so that quick action can be taken.
- **Strengthen resources:** This sector must be given the importance it deserves, in terms of finances and manpower.
- **Offensive capacity:** There is need to develop the offensive capabilities as well rather than being merely defensive.
- **Integrated cyber security command:** At present, we follow sector-specific policy of cyber security which hampers coordinated efforts. Therefore, we need an integrated cyber security command.
- **Strengthening cyber Legislation in the country.**

10. Considering the sophistication of cyber adversaries, it is imperative for India to focus on building a cyber-resilient environment. Discuss. Also, list some steps taken by the government to increase robustness of cyber security architecture in India.

Approach:

- Highlight the state of cyber-security in India.
- Emphasise upon the growing sophistication of cyber adversaries.
- Discuss how India's booming digital economy also makes it more vulnerable to cyber-attacks.
- List some of the initiatives taken by the government to strengthen the cyber security architecture in India.

Answer:

The spread of malware, misinformation and systemic cyber-attacks has become a huge challenge in recent times. In 2018, the F-secure report placed India at the 21st spot in the global tally with over 6.95 lakh cyberattacks. UBI Heist (2016), WannaCry ransomware (2017), PETYA ransomware (2017) etc. were some of the more prominent cyberattacks.

Sophistication of cyberattacks and data breaches:

- Cyber criminals are likely to use more sophisticated tools to take advantage of the **changing technological landscape**. For instance:
  - Attackers may implement Artificial Intelligence to deliver more targeted phishing messages.
  - It is anticipated that growing vulnerabilities found in **cloud infrastructure,** such as containers, and weak cloud security measures allows greater exploitation of accounts for cryptocurrency mining. This may lead to more damaging breaches due to misconfigured systems.
  - There are growing threats of **SIM swapping and SIM-jacking** which allow criminals to hijack a cell phone without the user's knowledge, making it difficult for consumers to regain control of their devices.
- The **malware types** used are getting increasingly complex, making their detection difficult for cyber security agencies.
- The **frequency of attacks,** their nature and the stature of the victim enterprises indicate the progressive sophistication of cyber adversaries.

Such attacks and data breaches are clear signals to escalate cybersecurity as a major governance issue, implying the **need for a cyber-resilient India:**

- India's security challenge in cyberspace depends upon the design and density of its digital ecosystem. Several **government initiatives** are aiming towards digitizing several vital sectors of the country. Flagship initiatives like 'Make in India', 'Start-Up India' and 'Digital India', as well as governance premised upon connectivity, will hinge upon safety of cyberspace in India.
- The booming digital economy in India hosts the world's second largest user base on the internet. There has been a tremendous growth in **digitally connected population** and IT spending in India to scale up the **use of technologies** like Internet of Things (IoT), Cloud Computing, Artificial Intelligence (AI) and Blockchain. Consequently, the integrity of India's cyber platforms will increasingly be subjected to threats and vulnerabilities in future.

Initiatives taken to strengthen cybersecurity architecture in India:

- **National Cyber Security Policy, 2013** provides the vision and strategic direction to protect the national cyberspace.

- **Institutional set up includes - National Cyber Coordination Centre (NCCC), National Critical Information Infrastructure Protection Centre (NCIIPC), Computer Emergency Response Team (CERT-In) etc.**
- **Cyber Swachhta Kendra,** provides a platform for users to analyse and clean their systems of various viruses, bots/ malware, Trojans, etc.
- **Organising Cyber Security Competition** like Global Cyber Challenge, etc. to find out the system vulnerabilities and getting prepared to tackle them effectively.
- **Bilateral agreements** with developed nations such as the US, Singapore, Israel, Japan, etc. to promote research and information sharing on cyber security.
- **Cyber Crisis Management Plan** (CCMP) for countering cyber threats and cyber terrorism has been developed.

Heartiest Congratulations to all Successful Candidates

Aditya Srivastava

16 in **TOP 20** Selections in **CSE 2023** from various programs of **Vision IAS**

Animesh Pradhan

Ruhani

Srishti Dabas

Anmol

Nausheen

Aishwaryam Prajapati

39 Selections in **TOP 50** in **CSE 2022**

Ishita Kishore

Garima Lohia

Uma Harathi N

SHUBHAM KUMAR

CIVIL SERVICES EXAMINATION 2020

DELHI

HEAD OFFICE
Apsara Arcade, 1/8-B 1st Floor, Near Gate-6 Karol Bagh Metro Station

MUKHERJEE NAGAR CENTER
Plot No. 857, Ground Floor, Mukherjee Nagar, Opposite Punjab & Sindh Bank, Mukherjee Nagar

GTB NAGAR CENTER
Classroom & Enquiry Office, above Gate No. 2, GTB Nagar Metro Building, Delhi - 110009

FOR DETAILED ENQUIRY
Please Call:
+91 8468022022,
+91 9019066066

enquiry@visionias.in /c/VisionIASdelhi /visionias.upsc /vision _ias VisionIAS_UPSC

AHMEDABAD BENGALURU BHOPAL CHANDIGARH DELHI GUWAHATI HYDERABAD JAIPUR JODHPUR LUCKNOW PRAYAGRAJ PUNE RANCHI

VISIONIAS
INSPIRING INNOVATION

Classroom Study Material

INTERNAL SECURITY

ROLE OF MEDIA AND SOCIAL NETWORKING

Sites In Internal Security Challenges

AHMEDABAD BENGALURU BHOPAL CHANDIGARH DELHI GUWAHATI HYDERABAD JAIPUR JODHPUR LUCKNOW PRAYAGRAJ PUNE RANCHI

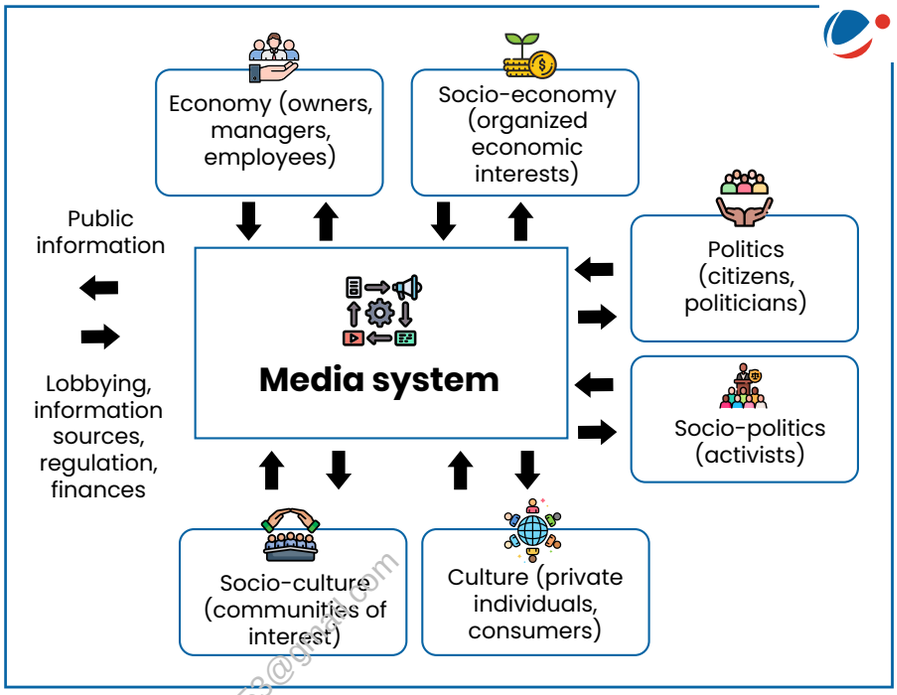
CONTENTS

1. Media

1.1. Introduction

Any **communication channel** through which any kind of information, news, entertainment, education, data, promotional messages etc. can be disseminated is called media.

Mass media refers to communication devices, which can be used to communicate and interact with a large number of audiences in different languages. Be it the pictorial messages of the early ages, or the high-technology media that are available today, mass media has become an inseparable part of our lives. Media can be broadly classified as:



- **Print Media** (newspapers, magazines, books and Brochures, Billboards, etc.).
- **Electronic Media** (news websites, social networking sites, mass SMS schemes, television, radio, cinema etc.).
- **New Age Media** (Mobile Phones, Computers, Internet, Electronic Books).

1.2. Role of Media in India

For a country like India, the backbone of its democracy and the propagator of its national interests remains the access to information and expression. It helps citizens to make responsible and objective choices, to promote accountability in its officials, to provide solutions for conflict resolution, and to also encourage diverse views of different people. This access to information has allowed the Indian media to play the role of **watchdog,** holding the government accountable in all its activities, and also functioning as a medium for expression for the ordinary citizens.

The role of media in a democracy like India, therefore, can be summed up as:

- **Media as an instrument of expression:** Media in exercise of freedom of expression is essential to communicate the thoughts, views, philosophy, ideals and activities.
- **Media as the Fourth Estate:** It acts as the bridge between the three institutions of the government (Legislature, executive and judiciary) and the people.
- **Educating people through media:** This is largely done by reporting of the news as well as the social commentary on these events.

- **Mass Media can also help in bringing change:** It can be instrumental in bringing about changes in the attitudes and habits of the masses. For example, dispelling the false notions around people suffering from diseases like leprosy, HIV/AIDS, Corona, etc. has been possible only through wide media campaigns.
- **Media promoting distribution of goods:** It drives the consumer choice and generates demand for goods and services through advertisements.
- **Role of Media in Nation Building:** It can aid public involvement through advocating issues of national importance and transferring knowledge, skills and technologies to the people. Awareness about various rural development programs, propagation of family planning could be spread by using the media.
- **Shape the perceptions** of government, influence public opinion, promote democracy, good governance as well as influence peoples' behavior and support people- oriented policies.

Following the globalization, the responsibilities of media have also widened. It has a role in preserving and pursuing the national interests of the state and highlighting its perspective along with the global issues. It has to examine the status of international relations and again to highlight the trouble spot at global level in lieu of global security.

1.3. National Security & Media

The media and national security policy of a nation have a strong connection in the contemporary environment. Television news in India, with far too many channels competes for viewership 24/7, and with the **'Breaking News'** sensation, sets the pace for the print media. The distinction between facts, opinions, and speculation has blurred into irrelevance.

Reconciling the roles of the media and the government

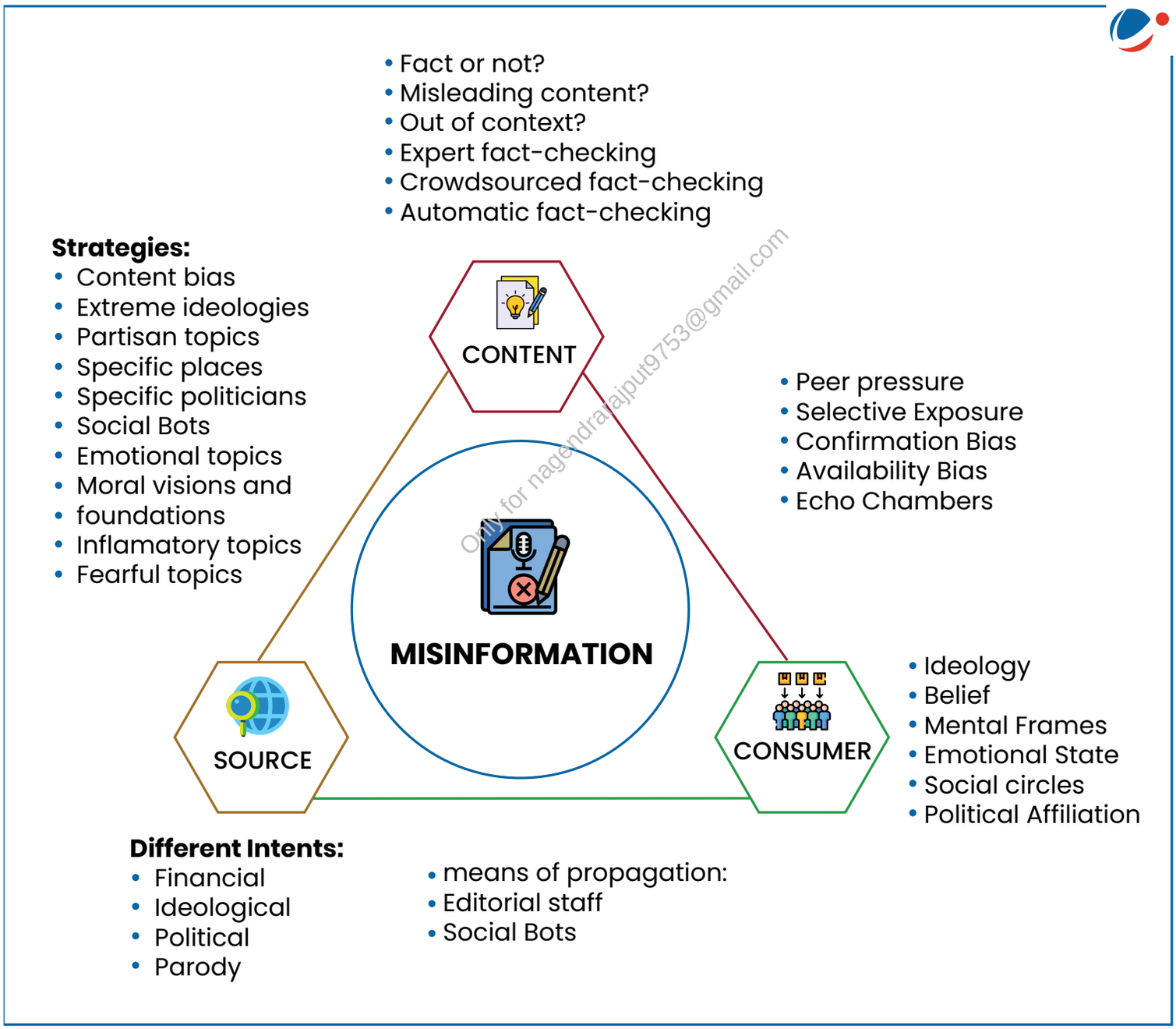
- The test of **"direct, immediate, and irreparable damage to our Nation or its people"** represents the test to determine when its is constitutionally permissible for a court to issue an injunction against the publication of information allegedly harmful to "national security".
- Freedom of expression also embodies the principle of editorial discretion and the role of the media to refuse publishing of information harmful to national security.

The connection between the media and national security policy is both direct and indirect. The perennial war of ratings of the TV channels has led the newspapers to try to outdo their visual media competitors in order to gain readership. Consequently, newspapers and TV channels report news in a manner that instigates outrage rather than increase awareness and initiate a debate. The threats posed by the media to the internal security include:

- The electronic media in particular has long since dropped the pretension of providing a public service, with senasationalisation of every news item without any verification of substance.
- Indian media is in no mood to apply brakes or observe self-restraint on its wayward and insensitive treatment of national security issues.
- Indian media's (especially electronic media) analysis of national security issues by groups of former diplomats, generals and academia's arm chair strategists distorts national security perspectives. All these gentlemen can only draw on their outdated experience and none of them are privy to latest inputs. Also in many cases, reticence is their first casualty after retirement.
- Indian TV anchors discussing national security issues do not have the political and strategic maturity

to discuss national security issues as their Western counter-parts do.

- Indian TV debates on national security issues tend to cut out development of contrary views and perspectives by imposing commercial breaks, or go hectoring themselves.
- The role of the media threatens national security when it obtains "unauthorized disclosures leaks" from officials inside the government, and decides to publish or broadcast it, without considering the security implications.
- The cut throat competition, especially in case of electronic media, has resulted in priority to exclusivity of coverage over **authenticity** of the news itself. This manifests in a lack of **culture of fact-checking,** resulting in dissemination of **fake news,** often having internal security implications.
- The media can also play a negative role in flaming communal tensions through their coverage of various issues. For example, the SC had to intervene to impose a pre-telecast ban on a programme " UPSC JIhad", partially aired on a news channel.



1.4. Existing Regulations and Restrictions

- The rights and responsibilities of the media are not directly enshrined in the written Constitution; however, **Article 19** of the Indian Constitution dealing with the freedom of speech and expression broadly highlights the powers and functions of the media as a body of information.
- **Articles 105(2) and 194(2)** allow the Indian Press to publish or report the proceedings of the parliament and the state legislatures.
- A number of press laws such as the **Press Council Act of 1978** that nominates bodies to govern press functioning in India and the **National Security Act of 1980** puts restrictions on the Indian press while reporting on issues that may need to be confidential and whose exposure may threaten the stability of the nation.
- The **Press Council of India** aims to preserve the freedom of the press and maintain and improve the standards of newspapers and news agencies in India. It has the **power to receive complaints** of violation of the journalistic ethics, or professional misconduct by an editor or journalist.

"The coverage of the Mumbai terror attack by the mainstream electronic media has done much harm to the argument that any regulatory mechanism for the media must only come from within", the Supreme Court 2012

Supreme court in its ruling after 26/11 slammed the TV channels for live coverage of the 26/11 Mumbai terror attack. "Any attempt to justify the conduct of the TV channels by citing the right to freedom of speech and expression would be totally wrong and unacceptable in such a situation. The freedom of speech and expression, like all other freedoms under Article 19, is subject to **reasonable restrictions.**

An action tending to violate another person's right to life guaranteed under Article 21 or putting the national security in jeopardy can never be justified by taking the plea of freedom of speech and expression.

- The Government has been able to restrict the media during emergencies and has imposed laws that diminish its freedom in a limited manner mainly to deal with national security related issues. Some examples include:
  - **Defence of India Act, 1962 –** It came into force during the Emergency declared in 1962 – the Sino India war. This Act aimed at restricting the Freedom of the Press to a large extent and in turn empowered the Central Government to issue rules with regard to prohibition of publication or communication which would undermine or threaten civil defence/ military operations, and also prevent prejudicial reports and prohibition of printing or publishing any matter in any newspaper that may contain such content.
  - **Civil Defence Act, 1968 –** It allows the Government to make rules for the prohibition of printing and publication of any book, newspaper or other document damaging to the civil defence of the country and its people.
  - **The Broadcasting Code –** It was adopted by the **Fourth Asian Broadcasting Conference** in 1962, highlighting major principles to be followed by the electronic media. The Broadcast Code was set

SC on media coverage of social issues.

- The media cannot make a religious minority the target of its attacks. The dignity of a community is as important as journalistic freedom.
- There is a need to strengthen the **self-regulatory mechanism** by the government in the media.

SC on Censorship of Content

- The general public interest supersedes the requirement to protect the individuality and expression of any artists
- A specific standard of censorship is required to be formulated in this regard to not curb the growth of an artist's individuality and freedom of expression.

up to govern the All India Radio, but the following key principles have also been followed by all Indian Broadcasting Organizations. The principles include:

- Ensuring the **objective** presentation of news and **fair and unbiased** comment, to promote the advancement of education and culture.
- Raising and maintain high **standards of decency and decorum** in all programmes.
- Providing programmes for the young which, by variety and content, will inculcate the principles of good citizenship.
- Promoting communal harmony, religious tolerance and international understanding.
- Treating controversial public issues in an impartial and dispassionate manner.
- Respecting human rights and dignity.

- **News Broadcasting Standards Authority –** It is an independent body set up by the News Broadcasters Association. Its task is to consider and adjudicate upon complaints about broadcasts.
- The Indian Broadcasting Foundation has also released **'Self-Regulatory Content Guidelines for Non-News and Current Affairs Television Channels',** after the critical broadcasting of the Mumbai terror attacks in 2008 that brought in media experts and journalists to review the coverage and revise the content of the Indian media.

1.5. Measures to tackle the threat

Considering the potential of media to harm the national security and health of a nation, following measures shall be undertaken to tackle the national threat:

- **Accuracy in reporting–**
  - It is the responsibility of TV news channels to keep **accuracy and balance,** as precedence over speed as usually expected.
  - If despite this there are **errors,** channels should be **transparent** about them. Errors must be corrected promptly and clearly.
  - Channels should also strive not to broadcast which is defamatory or libelous.

India's National Security Issues and Indian Media Record:

India's Nuclear Weapons Test 1998: The Indian media went berserk in politicising the issue. It chimed that there were no national security threats in evidence justifying it. Within seven months the Kargil War took place.

Pakistani Proxy War in J&K: The media has been totally irresponsible. India's strategic sensitivities are constantly ignored and there is a competition to adopt extreme liberalist views. One theme often stressed is of Kashmiri alienation. Had that been so, Pakistan by now would have inflicted a Bangladesh on India.

Kargil War: Instead of marshalling the nation into a cohesive force, the Indian media playing partisan political roles at the height of the war, were busy stoking controversies as to how it happened.

Agra Summit: The summit had more to do with India's national security interests than political diplomacy. The Indian Media went berserk in focusing and projecting General Musharraf's view point than advancing India's interests. What a comparison to the Pakistani journalists who utilised India's electronic media space to defend and advance their country's interests.

India's Military Mobilisation December 2001: Pakistan did not have to use ISI to spy on India's mobilisation efforts and moves of its strategic formations. The Indian media was doing the job.

Neutrality, Impartiality and Objectivity

- Media must provide for **neutrality** by offering equality for all affected parties, layers and actors in any dispute, or conflict to present their point of view.
- Though neutrality does not always come down to giving equal space to all sides news channels must strive to ensure that allegations are not portrayed as fact and charges are not conveyed as an act of guilt.

To ensure crime and violence are not glorified

- News channels should exercise **restraint** to ensure that any report or visuals broadcast do not induce, glorify, incite, or positively depict violence and its perpetrators, regardless of ideology or context.
- Specific care must be taken not to broadcast visuals that can be prejudicial or inflammatory. Equally, in the reporting of violence, the act of violence must not be glamorized, because it may have a misleading or desensitizing impact on viewers.
- News channels must ensure that no woman or juvenile, who is a victim of sexual violence, aggression, trauma, or has been a witness to the same is shown in television without due effort taken to conceal the identity.
- In reporting all cases of sexual assault, or instances where the personal character or privacy of women is concerned, their names, pictures and other details shall not be broadcast/divulged.

Privacy

- As a rule, channels must not intrude on private lives or personal affairs of individuals, unless there is a clearly established larger and identifiable public interest for such a broadcast.
- However, it is also understood that the pursuit of the truth and the news is not possible through the predetermined principle of prior permission; hence door stepping individuals or authorities for the purpose of news gathering may be used only in the larger purpose of public interest.
- Further, in the case of minors, in any broadcast that intrudes on their privacy, the channel should attempt, where possible, to seek the consent of the parent or legal guardian.

National security

- In the use of any terminology or maps, that represents India and Indian strategic interests, all news channels shall use specific terminology and maps mandated by law and Indian governments.
- News channels shall also refrain from allowing broadcasts that encourage secessionist groups and interests, or reveal information that endanger lives and national security.
- However, it is in the public interest to broadcast instances of breach of national security and loopholes in national security and reporting these cannot be confused with endangering national security.

Superstition and occultism

- News channels shall not broadcast any material that glorifies superstition and occultism in any manner.
- In broadcasting any news about such genre, news channels will also issue public disclaimers to ensure that viewers are not misled into believing or emulating such beliefs and activity.

- Therefore, news channels shall not broadcast "as fact" myths about "supernatural" acts, apparitions and ghosts, personal or social deviations or deviant behavior and recreations of the same.

Sting operations

- As a guiding principle, sting and under-cover operations should be a last resort of news channels in an attempt to give the viewer comprehensive coverage of any news story.
- News channels shall not allow sex and sleaze as a means to carry out sting operations, the use of narcotics and psychotropic substances or any act of violence, intimidation, or discrimination as a justifiable means in the recording of any sting operation.
- News channels will as a ground rule, ensure that sting operations are carried out only as a tool for getting conclusive evidence of wrong doing or criminality, and that there is no deliberate alteration of visuals, or editing, or interposing done with the raw footage in a way that it also alters, or misrepresents the truth or presents only a portion of truth.

Strengthening of Institutional Framework

- Giving Press Council of India powers to enforce its guidelines and to penalize newspapers, news agencies, editors, etc. for the violation of its guidelines.
- Government should consider granting **statutory status** to the News Broadcasters Association (NBA) which represents the private television news and current affairs broadcasters.
- Need for an **independent industry led body** to enforce core principles of media ethics like truth and accuracy, transparency, fairness and impartiality etc on a regular basis. The body should have powers to impose immediate financial costs for broadcasters and editors in case of violation of these principles.
- **Media Trials:** In a criminal trial, the prosecution and the accused have the right to a fair trial. Between free speech and fair trial, the borders are sometimes crossed and the rules breached, leading to devastating consequences to individuals and institutions. The 'tele-terror' should not be allowed to meddle with a trial in accordance with the law. The digital violence in itself is a breach of peace.

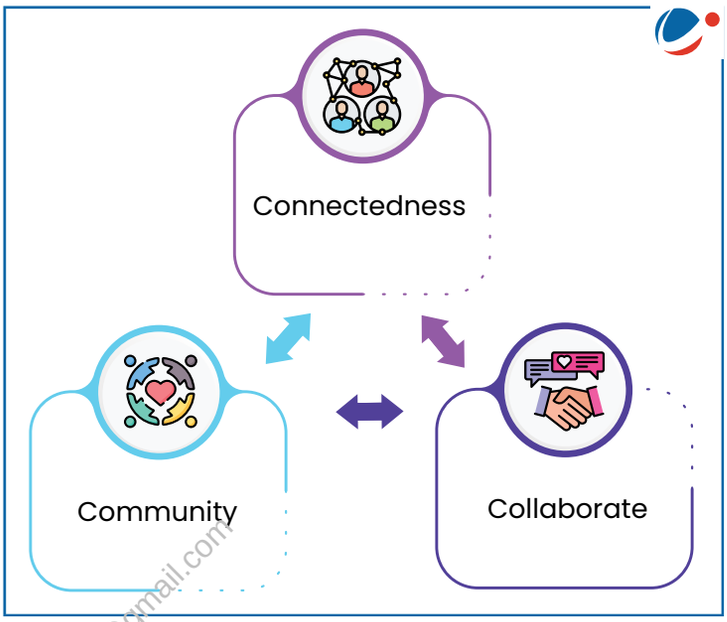
"The internet is the largest experiment involving anarchy in history. (...) It is a source for tremendous good and potentially dreadful evil, and we are only just beginning to witness its impact on the world stage."

– Eric Schmidt, Executive Chairman, Google and Jared Cohen, Director, Google Ideas

2. Social Media

2.1. Introduction

Social media is best understood as a group of new kind of online media, which share most or all of the following characteristics:



- **Participation:** Social media encourages contribution and feedback from everyone who is interested. It blurs the line between media and audience.
- **Openness:** Most social media services are open to feedback and participation. They encourage **voting, comments and the sharing** of information. There are rarely any barriers to accessing and making use of content, password-protected content is frowned on.
- **Conversation:** Whereas traditional media is about "broadcast" (content transmitted or distributed to an audience) social media is better seen as a **two-way conversation.**
- **Community:** Social media allows communities to form quickly and communicate effectively, sharing common interests.
- **Connectedness:** Most kinds of social media thrive on their connectedness, making use of links to other sites, resources and people.

2.2. Social Media vs Social Networking

Social Media and Social Networks in actual terms differ as social media is a **communication** channel that transmits information to a wide audience and is usually a one-way street, while social networks facilitate the act of **engagement** between like minded people, groups or communities.

2.3. Types of Social Media

There are several kinds of social media:

- **Social networks:** These sites allow people to build personal web pages and then connect with friends to share content and communication.
- **Blogs:** a blog is an online journal where the entries are written in a personal, conversational style. They are usually the work of an identified author or group of authors
- **Wikis:** These websites allow people to add content to or edit the information on them, acting as a community document or database. Example- Wikipedia
- **Forums:** Areas for online discussion, often around specific topics and interests. Each discussion in a forum is known as a 'thread', and many different threads can be active simultaneously. This

makes forums good places to find and engage in a variety of detailed discussions. One **major difference between forums and blogs** is that the Blogs have a clear owner, whereas a forum's threads are started by its members.

- **Content communities:** They organize and share particular kinds of content. Here, you have to register, you get a home page and then make connections with friends. The most popular content communities tend to form around photos (Flickr), bookmarked links (del.icio.us) and videos (YouTube).
- **Micro-blogging:** Social networking where small amounts of content (updates) are distributed online and through the mobile phone network. Example- Twitter.

The use of social media for policing may be seen by many initiatives like:

- Delhi Traffic Police using platforms like Facebook and Twitter to ease handling of traffic related issues,
- Delhi police online FIR facility for lost articles,
- Indore police using the medium to track criminal activity
- Bengaluru police twitter handle selected for "Twitter Samvad".
- Social Media Labs Project by Maharashtra Police tracks activity on social media to anticipate and handle sudden flare ups

2.4. National Security & Social Media

Social Media can represent an effective opportunity to preserve national security and/or reach the strategic interests of a state if used properly by civil institutions and, in particular, by security services and/or information security services. Besides, these tools "can be used by governments for **content creation, external collaboration, community building, and other applications**" and that "failure to adopt these tools may reduce an organization's relative capabilities over time".

Security and law enforcement agencies can use social media platforms in the following ways for internal security:

- To use data available freely on social media platforms to **gauge the mood** of citizens on issues, **predict patterns** and possible flash points of disturbances, and prevent and react to cyber crimes
- To build **actionable intelligence** which may support human intelligence efforts which could be shared across agencies, with built in safeguards to ensure that there is no encroaching upon the privacy of citizens.
- **Warning and Trend Prevision Tool-**
  - The ability to forestall future strategic and tactical contexts is of paramount importance in order to reduce the possibilities to be caught by surprise by threats and increase the resilience to them.

Negative Impact of Social Media on Democracy

- Foreign Interference: It has been used as an information weapon to influence public sentiment in elections by external state actors. For ex. the setting up and promotion of fake pages on Facebook by Russian entities in US 2016 election.
- Fake News: It has allowed criminal actors to launch misinformation campaigns and incite violence.
- Echo Chambers: It creates bubble where people only see viewpoints they agree with, strengthening the preferred narratives and rejecting the information that undermines it, thereby creating a polarised society.
- Political Harassment: As more countries write laws that attempt to criminalize online discourse, the risk grows that states use their power to intimidate their critics. That could have a chilling effect on speech.
- Unequal Participation: Vulnerable populations could end up ignored, and fringe groups could appear mainstream.

Institutional Communication Tool-

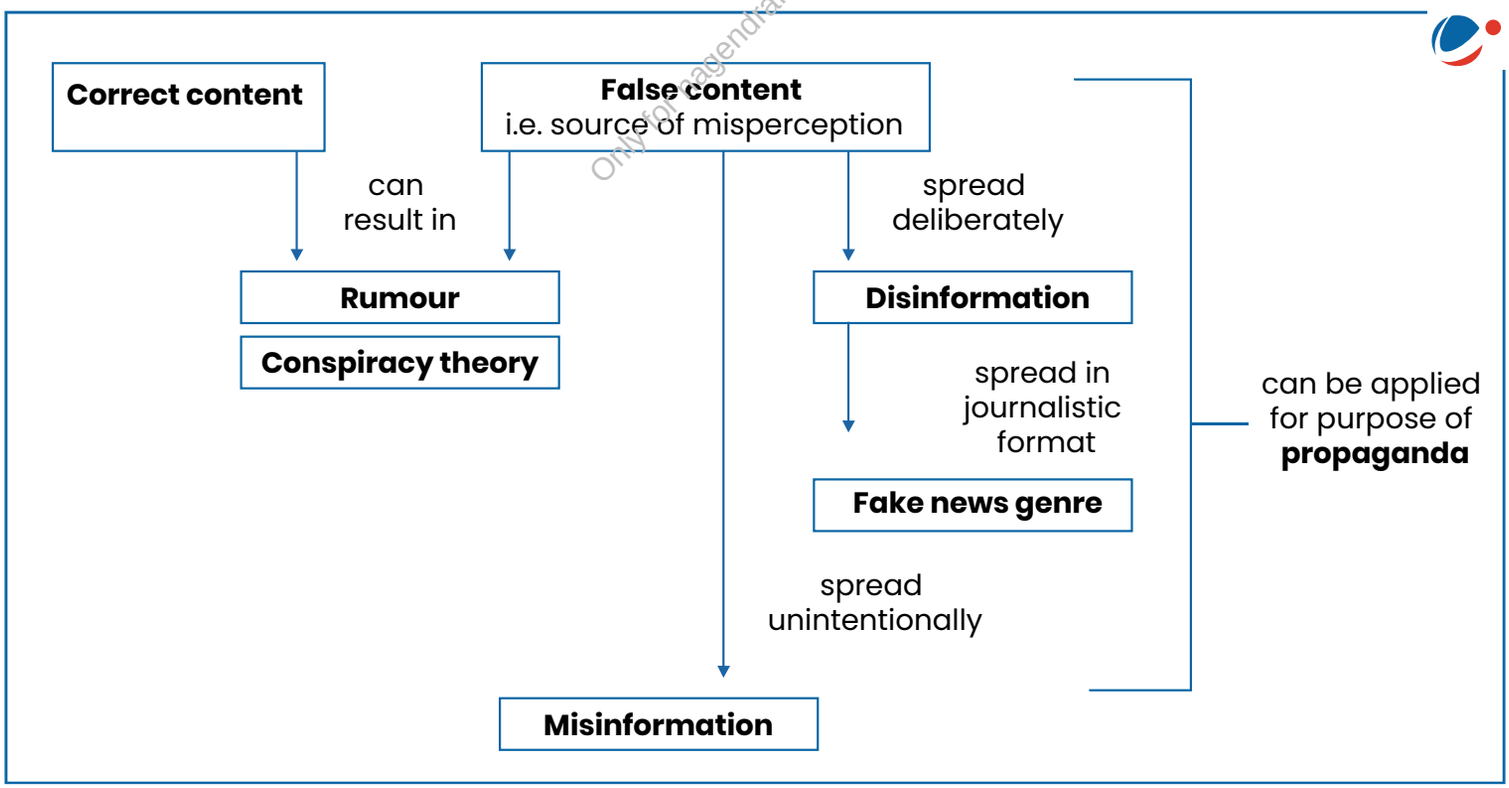
- A state has to reach **Information Superiority,** referred to as an advantage over the adversary in IT and decision-making, if they really want to guarantee high competitiveness and efficiency standards, protect their own strategic interests and effectively counter threats to national security.
- Social Media can help reach this kind of competitive advantage since they increase the **agility and flexibility** of the information sharing procedures and accelerate the decision-making process.
- to inform and engage with citizens to build secure communities which share information;
- to ensure presence to combat misuse of social platforms to spread malicious rumors which may trigger problems for internal security and law and order, and prepare standard operating procedures for times of emergency;

Influence, Propaganda and Deception Tool-

- The use of Social Media allows not only to communicate, share or capture information, analyze sociopolitical dynamics and anticipate economic-financial trend, but also to describe events, model reality, influence the perception of a certain situation, a specific issue or a person, and influence choices and behaviors. For example, the use of fake social media profiles to influence public opinion towards Presidential candidates by external state actors was witnessed in the 2016 US elections.

2.5. Threat to Internal Security

Social media poses challenge for democracies because the channels such as social networks and blogs present powerful tools to spread information to the masses. Few examples to remember are the Moldavian twitter riot, the London riots, the Iran elections, the WikiLeaks disclosures, or the Arab freedom movements. The efficient use of the tools provided by the new media is the new military power because electronic media and social media are the most effective and powerful means of mass motivation.



For the Indian government, the internet remains the chosen platform for socio-economic empowerment schemes, which also makes India uniquely dependent on internet platforms for its development while, at the same time, it heightens the risks of India's vulnerabilities.

Challenges to internal security through Social Media

Rise in rate of communal violence due to fake news or videos shared on social media: For instance, mob lynchings and attacks on the migrant population.

Anti-national groups/elements like some youtube channels operating from Pakistan to spread disinformation and fake news.

Use by Terrorist groups like ISIS during its peak spreading propaganda material in Hindi, Tamil, etc.

Cyber Attacks: Social networks have become a great vector for Trojans like mobile banking **SOVA Android Trojan.**

Deep Fakes: Advances in Artificial Intelligence (AI) and Machine Learning (ML) have enabled computer systems to create synthetic videos or deep fakes to sow the seeds of polarisation, amplifying division in society, and suppressing dissent.

Data Colonisation by social media global corporations which can be manipulated against India.

Criminal Activity and Money laundering through social media platforms.

Virtual Community is the means of attracting potential members and followers like **Lone wolf attackers.**

Terrorism:

- Social Media are more and more used by terrorist organizations as tools for **ideological radicalization, recruitment, communication and training.**
- The rapid expansion and development of social media can be used to cause problems by propagating certain ideologies, mobilizing and organizing people.

Protest Movements and Revolution:

- Social Media constitute an asset of great importance both for protest movements and for revolutions. Rebels and revolutionary groups turn to such tools to better organize and spur masses to action, to arrange protest or struggle activities and manage their tactical and operational aspects.
- It has a potential for disrupting public order, either involuntarily through the unchecked spread of rumors, or deliberately through the propagation of misinformation with the intent of creating enmity between groups.

Criminality:

- Criminal organizations use Social Media as **support, communication and coordination tools** to conduct their illicit activities.
- This kind of illicit activities can be either purely information ones (i.e. spreading child pornography with fee, "virtual" identity thefts, phishing, spread of viruses, Trojans, worms, etc.), or "traditional" ones (i.e. drug smuggling, human trafficking, money-laundering, transfer of documents from industrial espionage).

- Mobile phone technology provides easy and instant digital camera and video facilities, and this can be used maliciously.
- Cases of cyber bullying, misuse and corruption of personal information, the posting of material about an individual by third parties, often of a malicious nature, and publishing of material involving others, without their consent, which can be embarrassing or worse.

War:

- According to a recent **NATO provisional study,** future conflicts will occur in more and more connected environments, which will be characterized by the use of new communication and information technologies, Social Media included.
- The media networks are regularly hacked by enemy countries to spread false information and to recover classified data. Recently hacking of New York Times and Twitter servers by Syrian agencies was in news. Similarly, the US and China continue to exchange blows in the field of hacking.

Silent circle's applications: A threat

- **Silent Phone:** Encrypted voice and video calls on mobile devices. it can be used with Wi-Fi, EDGE, 3G or 4G cellular anywhere in the world.
- **Silent Text:** Encrypted text messaging with 'burn notice' feature for permanently deleting messages from device registries.

2.6. Key Issues

2.6.1. Digital Media Regulation

Digital Media can be broadly classified into the following:

1. Social Networking Sites like Facebook, and microblogging websites like Twitter etc.

2. Over the top (OTT)platforms

1. Social Media Regulation

Given its characteristics to potentially give **"voice to all",** immediate outreach and 24*7 engagement, Social Media offers a unique opportunity to governments to engage with their stakeholders especially citizens in real time to make policy making citizen centric. Many governments across the world as well many government agencies in India are using various social media platforms to reach out to citizens, businesses and experts to seek inputs into policy making, get feedback on service delivery, create community based programmes etc.

However, this has also created its own set of issues like:

1. **Lack of privacy:** Stalking, identity theft, personal attacks, and misuse of information are some of the threats faced by the users of social media.
2. **Cyber bullying:** People can misuse social media platforms to spread rumors, share videos aimed at destroying reputations and to blackmail others.
3. **Fake news:** While everyone becomes a source of information, hardly anyone adheres to the strict standards of scrutiny required for the information to be passed on as news. This results in a barrage of fake news with real life consequences.
4. **Trolling:** According to the Research by Amnesty International,

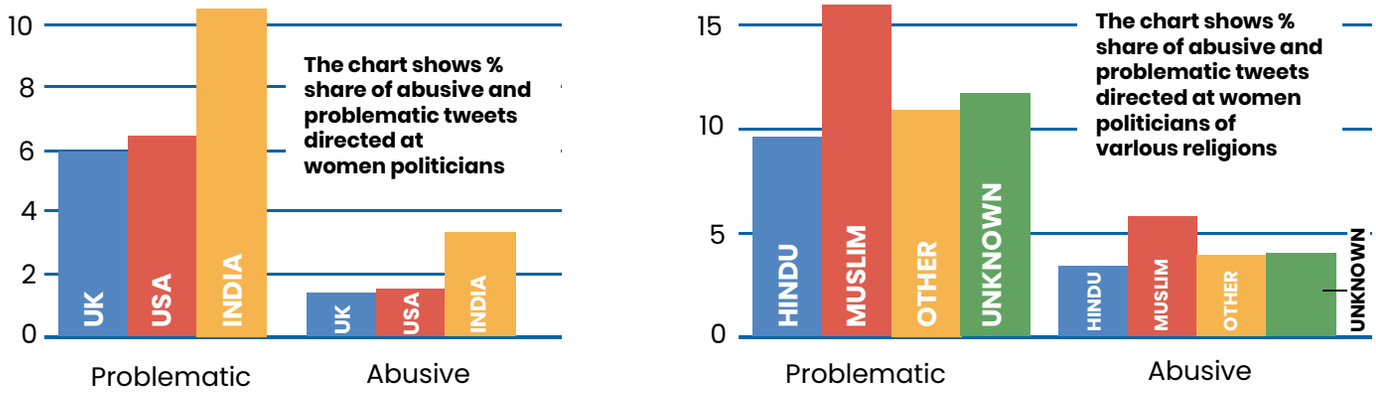
- Women are targeted with abuse online not just for their opinions – but also for various identities, such as gender, religion, caste, and marital status.
- Indian women politicians face substantially higher abuse on Twitter than their counterparts in the U.S. and the U.K.
- Women from marginalized castes, unmarried women, and those from non-ruling parties faced a disproportionate share of abuse.

5. **Accountability issues -** Challenges with respect to fixing the liability of intermediaries.
6. **Jurisdictional challenges -** Complications in jurisdiction as Facebook etc. operate as subsidiaries of foreign internet companies with their servers located outside India.

7. Anonymity - Police officers have expressed concern over multiplicity of fake profiles.

Softer targets

Women politicians from India faced significantly more abusive and problematic tweets compared with their counterparts in the U.S. and the U.K. Muslim women politicians, in particular, faced more such tweets than others



2. Over-the-Top Platforms

The Ministry of Information and Broadcasting ("MIB") has been undertaking the ginormous task of **regularizing and certifying** the content available on various entertainment platforms and digital media in general, more particularly referred to as the over the top platforms ("OTT"). MIB would soon call for talks with the major stakeholders of the prevalent OTTs, including **Netflix, Amazon Prime Now, Hotstar etc.** as also with members of civil society, technical community, media and legal experts, in order to discuss and formulate a **concrete mechanism** of certification and regularization of the content available on such OTTs.

This requirement for the MIB to formulate regulations to certify and regularize the content available on OTTs has stemmed from the **displeasure of certain groups** in relation to certain web series (which are currently being streamed on such OTT platforms) as **'violent' and 'vulgar'.** The **High Court of Karnataka** has also suggested to the Central Government to consider setting up a mechanism of certification and regularisation of the online content.

Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 mandate social media platforms to exercise greater diligence in content moderation, ensuring online safety by promptly removing inappropriate content.

- Users must be educated about privacy policies, avoiding copyrighted material, defamatory content, or anything that threatens national security or friendly relations.
- The 2023 Amendment to these rules states that online intermediaries, including social media platforms like Facebook and internet service providers like Airtel, must prevent the spread of inaccurate information about the Indian government.
- However, the **implementation of amended provisions was recently halted by the Supreme Court.**

2.6.2. Media Trials

Media trial describes the impact of television and newspaper coverage on a person's reputation by creating a perception of guilt irrespective of the verdict in a court of law.

There has been **no legal system** where the media is given the power to try a case. Every coin has two sides so is the case with media trials and journalism, at certain instances journalist portrays a **pre-decided image** of an accused thereby tearing his/ her reputation that can eventually affect the trial and the judgment, henceforth trial by media.

Famous Examples

There have been quite infamous cases as well that outraged the public and impacted the Judiciary such as **The Jessica Lal case(2010)** where the media rejoiced over their efforts in bringing justice to Jessica Lal and the trial court had acquitted the accused of all the charges. **The Priyadarshini Mattoo case (2006)** where a law student was raped and murdered and the judgment of this case was suspected to have been influenced by Media Trial.

There are grounds which make the attention of the media around certain cases high, which include:

1. Cases could involve **children** or they could be so **gruesome** that it shakes the collective conscience of the society.
2. Cases involving celebrities either as victims or as accused.

Judges and judicial officers are not free of faults and can be **"subconsciously influenced"** by media trials or media publicity. Therefore, it becomes necessary to regulate media publicity while the trial is going on or pending

2.6.3. Data Localisation

What is it?

- Data localization is a concept that the personal data of a country's residents should be processed and stored in that country. It may restrict flow entirely or allow for conditional data sharing or data mirroring (in which only a copy has to be stored in the country).
- There is a growing perception that data localization will aid countries asserting sovereignty in digital domain, ensure informational security of its citizens & fare better in governance (as it goes digital.

Need for Data Localisation

- Economic development of the country: Data is the new oil, an economic resource, fueling the 4th Industrial Revolution.
  - Digital data in India to increase from 40,000 PetaByte (PB) in 2010 to 2.3 million PB by 2020 - twice as fast as the global rate. If India houses all this data, it will become 2nd largest investor in the data centre market and 5th largest data centre market by 2050. This will give significant push to AI led economy in India.

Measures towards Data Localisation

- The **Digital Personal Data Protection Act 2023** brings into effect data localization requirements – stipulating that sensitive personal data must be stored within India, thereby placing a geographical boundary on where certain types of data can be stored and processed
- A similar clause was incorporated in Government's draft e-commerce policy, which recommended localization for "community data generated by users in India from various sources including e-commerce platforms, social media, search engines etc."

- India has 2nd highest FinTech adoption rate amongst major economies in the world. Data localization would give a push to domestic production of high value digital products.
- Domains of cloud computing, data analytics etc. can become major job creators in future.
- There is a push among government department to use AI tools and attempt a predictive approach to policy making. With data localization, there is a scope of greater access to 'public data' collected by companies (e.g. traffic data collected by like Uber, street level data collected by Google Maps) for the Government.

- Increase India's tax revenue: Extensive data collection & processing by technology companies, and unfettered control of user data has allowed them to freely monetize Indian users' data outside the country without paying any taxes.
  - Localization would lead to a larger presence of MNC's in India overall, through local offices, and increase tax liability and open more jobs.
  - Data localization is supported by domestic companies like PayTM and PhonePe as it will level the playing field, currently rendered unequal due to differences in tax liabilities of international companies and those having permanent establishment in India. E.g. Google India tax dispute over advertisement revenue under litigation in court.
- Maintain data sovereignty & citizens' data privacy: With data stored in remote servers, the accountability of service providers (like Google, Facebook etc.) reduces as it is outside the purview of Indian regulatory authorities. With data localization, regulatory oversight on end-use of data will improve and business jurisdiction related loopholes will be plugged. E.g. Facebook shared user data with Cambridge Analytica to influence voting.
- Issue of national security: Data localization will help law enforcement agencies to get access to user data for investigation and prosecution
  - Currently, companies are dependent on Mutual Legal Assistance Treaties (MLATs) to obtain data from US companies leading to delays and legal challenges in foreign jurisdictions.
  - In many countries like US, tech companies are legally barred from disclosing data to foreign law enforcement agencies.

Before universalizing the policy of data localization, the Government needs to provide a push to local capabilities in data storage and processing

- Infrastructure status to data centres/server farms
- Adequate physical infrastructure (energy, real estate and internet connectivity) for setting up such centres

India should put in place in a cybersecurity law to ensure protection of private data of citizens.

2.7. Available Checks and Balances: Regulations

The way in which the internet allows data to be produced, collected, combined, shared, stored, and analyzed is constantly changing. Police projects like **Social Media Labs** depend entirely on information available on public platforms and hence authorities must anticipate contestations to what constitutes public data in times ahead.

The government is working on a policy which is aimed at keeping a hawk's eye vigil on the social media to check if it is being "misused" to conspire against India and spread anti-national propaganda- a regulatory framework for social media and online content. At present, there is only **a set of "do's and don'ts"**

for the social media which needs to be graduated to full-fledged guidelines that should be adopted on such a network.

Supreme Court has also expressed its concern for uncharitable comments, trolls and aggressive reactions on social media platforms on almost every issue, including judges and judicial proceedings. As use of social media evolves, for security and law enforcement agencies, questions regarding 'relevancy' of such data, and its 'admissibility' etc. will also be raised.

Steps taken by India

- **IT (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2023** established **PIB's fact-checking unit.**
- **Delhi Declaration of UNSC Counter-Terrorism Committee** flagged concerns over increased use of cyberspace and other Information Communication Technologies (ICT), including social media.
- **Banning/blocking anti-national** like recently 6 YouTube Channels were banned by PIB.
- **Strengthening the existing infrastructure:** e-Surveillance Projects like NATGRID, CERT-In, Central Monitoring System (CMS), Internet Spy System Network and Traffic Analysis System (NETRA) of India, National Critical Information Infrastructure Protection Centre (NCIPC) of India etc.

Under the **existing legal frameworks, Sections 69 and 69(a) of IT Act 2000** empowers the government of India to:

- Issue directions for **blocking of information** for public access and to issue directions for interception or monitoring or decryption of information through any computer resource when circumstances threaten public order, defence, security, sovereignty and integrity of India, or friendly relations with other states or to prevent incitement to the commission of any cognizable offence relating to the above circumstances.
- Article 69 (b) of the IT Act 2000 empowers agencies of the government of India, in this case the Dept. of Electronics and Information Technology, "to authorise to **monitor and collect traffic data or information** through any computer resource for cyber security" for cyber incidents and breaches.

2.8. Measures to Tackle the Threat

The nature of the medium is such that it has raised valid questions as to whether regulation is possible without infringing on the fundamental rights of the citizen relating to freedom of speech and privacy. Due to its characteristics, its constituents, its contents and its evolving power, Social Media cannot be controlled, censored or shut down. Social media has to be understood and adopted.

- **Institutionalise the blueprint for a National Social Media Policy:** The National Cyber Security Policy needs to be revised to include social media challenges which are distinct from the cyber security threats.
- Implement and institutionalise the Framework of Guidelines on social media engagement for the government organisations with the following elements:
  - Objective: Why an agency needs to use social media
  - Platform: Which platform/s to use for interaction
  - Governance: What are rules of engagement
  - Communication Strategy: How to interact
  - Pilot: How to create and sustain a community
  - Engagement Analysis: Who is talking about what, where and what are the main points of conversations

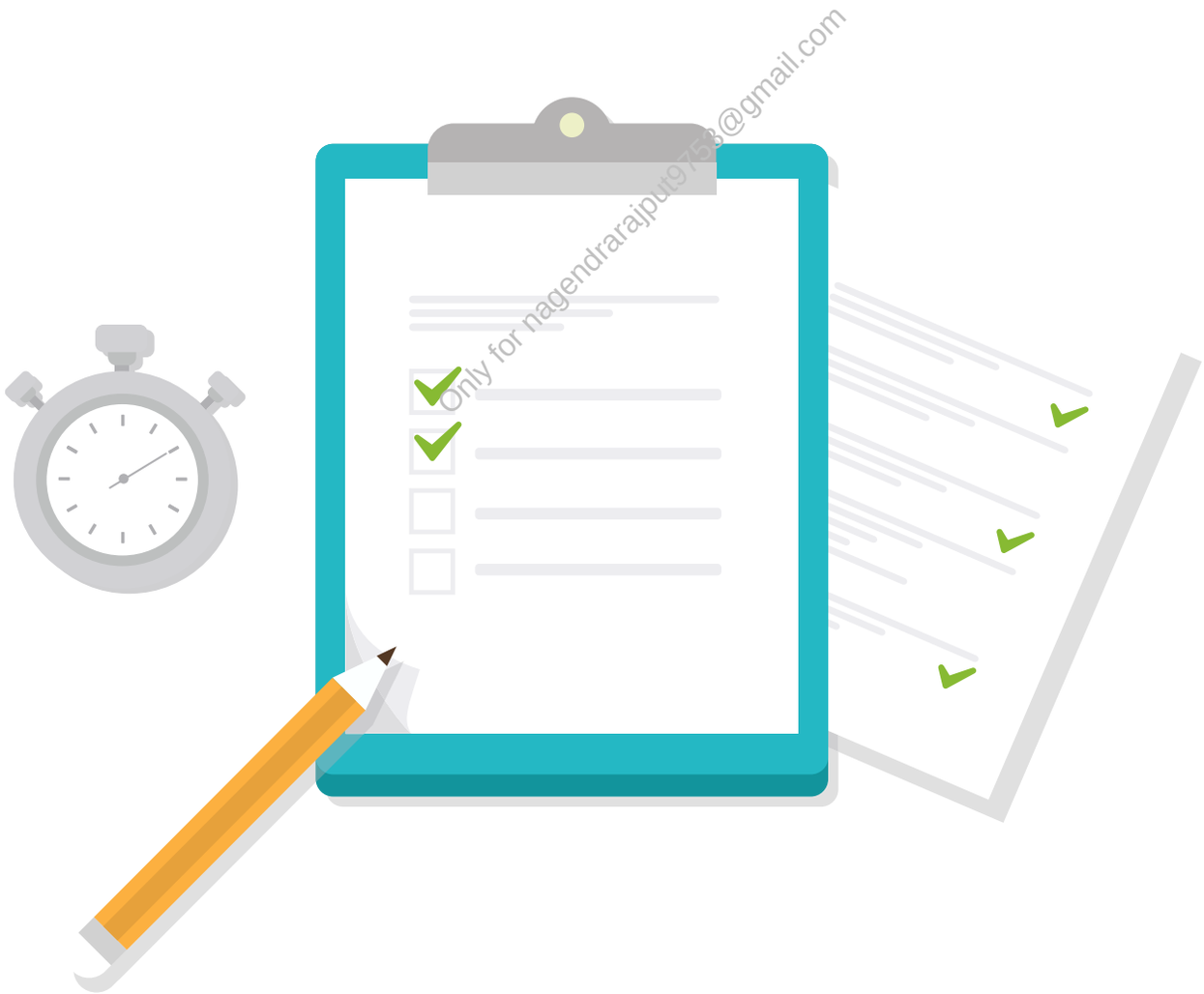
- Institutionalisation: How to embed social media in organisation structure

- Empower agencies, build talent, and use specialists: If the medium is to be adopted into daily practice by all personnel, then agencies must be empowered technically, legally and financially to use the medium to their specific purposes.
- Need a code of practice on disinformation: In line with the code by EU, it should allow platforms and agencies to take action in 5 areas:
  - Disrupting advertising revenues of certain accounts and websites that spread disinformation;
  - Making political advertising and issue based advertising more transparent;
  - Addressing the issue of fake accounts and online bots;
  - Empowering consumers to report disinformation and access different news sources, while improving the visibility and findability of authoritative content;
  - Empowering the research community to monitor online disinformation through privacy-compliant access to the platforms' data.
- The authorities can use the same medium to provide correct information and nip rumors in the bud. Existing technologies and laws provide sufficient leeway to the authorities to effectively monitor internet traffic, including social media, in real-time, but are under-utilized for a variety of reasons, largely to do with coordination.
- Social media analysis generated intelligence or **SOCMINT** is being developed as a successful model in many countries abroad to isolate hotspots or subjects that go viral and is used as a predictive tool. India too is looking at these models, but is still at the stage of experimentation, trial and error.
- We need more social media pilot projects across the country to develop a **truly credible data base** and this will require huge **investments** in terms of both infrastructure and human resource. We also need to work on network availability constraints, language barriers and, most importantly, organizational adaptability in terms of this new medium.
- We need to make people aware that the internet is not, in reality, a private place. The citizens should be guided of the advantages and of the risks of social networking sites, and provided an overall awareness, particularly to the young and vulnerable, about the need to be cautious in what they do online.
- From a **corporate perspective,** a revised security model which takes into account the sharing of information across social networks is necessary. There are risks in the use of and social networking software, though these are often not well recognized.
- A strengthening of legislation designed to **protect personal information.**
- Working to define and then to **protect data ownership rights in a web-based environment.**

The unique way that the internet continually improves in response to user experience is driving innovation on an unprecedented scale. Social media is developing in response to the appetite for new ways to communicate and to the increasingly flexible ways to go online. Its future direction is impossible to predict. What is beyond doubt is that social media – however it may be referred to in the future – is a genie that will not be disappearing back in to its bottle.

3. UPSC Mains Previous Years' Questions

1. 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. (2017)
2. Use of internet and social media by non-state actors for subversive activities is a major security concern. How have these been misused in the recent past? Suggest effective guidelines to curb the above threat. (2016)
3. 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? (2015)
4. "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. (2014)
5. What are social networking sites and what security implications do these sites present? (2013)



4. Vision IAS Mains Previous Years' Questions

1. The Supreme Court of India on the reckless media coverage of the 26/11 attacks noted that - "By covering the attack live, the Indian TV channels were not serving any national interest or social cause. On the contrary, they were acting in their own commercial interests, putting national security in jeopardy." In the light of the above observation, mention the principles and concerns that mass media should keep in mind while reporting sensitive and dangerous issues.

Approach:

The concerns indicated should be comprehensive, covering the aspects of impartiality, objectivity, sensitivity, privacy and national security. There is no need to go into a criticism of media in Mumbai terror attacks. The statement is only to highlight the importance of sensitivity in media reporting.

Answer:

Media, due to its power to influence the decisions of others and its role of information, education and communication, is considered as the fourth pillar of democracy. Hence, it becomes necessary that media follows certain principles of self-regulation so that it does not create, intentionally or unintentionally, problems for national security and law and order. Some important principles to be followed by the media are:

1. **Impartiality and objectivity in reporting:** Viewers of 24-hour news channels expect speed but that should not be at the cost of accuracy and balanced reporting. If errors in reporting have been made, they should be promptly admitted and corrected.
2. **Ensuring neutrality:** Equal opportunity must be given to all parties and actors to present their point of view. Neutrality does not mean giving equal space to all sides but it must be ensured that allegations are not portrayed as facts.
3. **No glorification of crime and violence:** Media should exercise restraint to ensure that any report or visual broadcast do not induce or glorify violence. Specific care must be taken not to broadcast visuals that can be inflammatory.
4. **Special care in cases pertaining to women and children:** In reporting cases of sexual assault or other cases involving privacy of women, their personal details should not be divulged. The identity of victims of child abuse and juvenile delinquents should be kept secret.
5. **Refrain from obscenity:** News channels must ensure that they do not show nudity or use sexually selective language.
6. **Respect individual privacy:** Channels must not intrude into personal affairs of individuals unless there is a clearly established larger and identifiable public interest.
7. **Should not endanger national security:** News channel should refrain from allowing broadcasts that encourage secessionist groups and interests. They should not reveal information that endangers lives and national security.
8. **Refrain from sensationalizing:** Media should take care that they do not indulge in sensationalizing news to gain more TRP. Special care is needed in instances of communal violence and sectarian conflicts to ensure that biased and prejudicial reporting is not done.

The Supreme Court's observation should act as an early warning to the media, which has been blinded by the need for greater audience and TRP. Self-regulation is the best form of regulation, especially in case of media. Hence media should try to stick to above principles so that its freedom remains ensured.

2. "While social networking sites have created a seamless and interconnected platform for communication, they have also created many challenges for our internal security". Comment.

Approach:

Justify the statement in the question in brief, citing how social media has broken down barriers of communication in modern era. Thereafter, one should highlight some of the challenges posed by misuse of social media to internal security. End the answer with a brief description of challenges and steps that should be taken by the government with regards to this problem.

The biggest positive of the social networking sites is that anybody can freely access them and use them for self-expression. Social networking site have reduced the communication barriers among the people. Many organisations are known to use social media strategies to reach out to customers and peers quite successfully. Even the governments have been using social media for broadcasting information about schemes and programmes to a great effect.

While at the same time the biggest danger lies in the possibilities of misuse of these sites from within or across the borders by anyone, either individually or through organized means. These sites are a store house of personal information and mass dispersion of information both; hence, there misuse can pose major security threats.

Social security sites posed major internal security threats in past

1. **Misuse of social media sites to ignite communal passions:** Intelligence bureau Chief Asif Ibrahim in 2013 pointed out that misuse of social media to fan communal tensions was the biggest threat to internal security, giving the example of a video that was circulated to incite communal violence in Muzzaffarnagar. Hand of Indian Mujjahidden was suspected in the same.
2. **It can cause mass panic, confusion and spontaneous reactions through misinformation:** The unprecedented cyber terrorism unleashed against people from North-East triggered big exodus within the country, with the north-eastern people fleeing major areas in Karnataka, Tamil Nadu, Maharashtra. All the sites were found hosting inflammatory and hateful content against people from north east inciting violence against them.

Why have these sites been able to pose a threat to internal security? The Problems:

- Proxy servers and virtual private network services which conceal the user identity operating from a number of countries appear to have been used for inciting passions and spreading misinformation.
- Google, you-tube, Twitter and Blogspot.com, do not show willingness to share the IP addresses of the users and their information directly who indulge in cyber terrorism. They request the governments to approach them through US government as they function under US IT laws, although India has a **mutual legal assistance treaty** with them.
- Google was more cooperative and any content which could incite violence was already blocked on it, but other sites like twitter refused to remove a major chunk of the inflammatory content, siting that inflammatory content was outside the jurisdiction of the country.

The government finds itself in a new information battlefield with no contingency plan, for the moment. Impulsive reaction was an immediate crackdown but, India has become second highest user of facebook., this is an audience that the government should reach out to, along with keeping a track that no population become victims of cyber-attacks.

3. While social media is being increasingly used to instigate communal riots and create social tensions, any effective strategy to check its misuse must balance security concerns and individual rights. Discuss in the context of recent developments in India.

Approach:

- Introduce answer with commentary on use of social media for creating tension in society.
- Discuss the restriction imposed by government.
- Comment on the Supreme Court judgment on Section 66A of IT Act.
- Suggest measure to balance the individual right and public order.

Answer:

In recent years, the social media has been increasingly used (in India) to instigate communal and social tensions. Law enforcement agencies have witnessed a worrying trend in last few years where social media posts and circulation of doctored audio-visual material over social networking site led to communal incidence.

- Riots in **Muzaffarnagar,** exodus of people from **North-East** from southern states are some of the events that highlight the threat from social networking sites. Circulation of inflammatory audio-visual material was the prime factor in these incidences.
- In response there is tendency among law enforcement agencies to impose additional restrictions on what is said and propagated on the social media. Any strategy to check the misuse of potential threats from the social networking site may lead to curtailment of fundamental rights guaranteed in constitution. Indian government amended the Information Technology Act (IT Act 2000) in 2009 to include section 66A aimed at checking misuse.
- However, its blatant misuse led to denying rights essential for healthy democracy. **The Supreme Court of India** recently passed a judgment declaring the section as unconstitutional. The case highlights the importance of a proper balance between civil liberties, individual human rights, and the responsibility of the state to maintain peace and order.
- It is not a simple case of misuse of law. In fact, the law suffers from the vice of non-application of mind. A bare reading of the section reveals how vaguely worded it is. It prescribes a maximum punishment of a prison term of 3 years with fine for sending information that is "grossly offensive" or has "menacing character" and for sending e mails causing "annoyance or "inconvenience" to the recipient.
- However, information technology has been recurrently exploited to harass or create public disorder cannot be denied. Section 66A has proved to be a useful remedy, particularly in situations of sensitive nature concerning religious and communal sentiment; for instance the episode of the exodus of north-east students from Bangalore where the Police Authorities were forced to take recourse to section to avoid spreading of rumours to incite violence against persons of the North Eastern community.
- Such instances where religious and communal harmony have been disrupted by publishing/ transmitting inflammatory content in the form of texts, mails, posts, etc. have to undoubtedly be deemed as "grossly offensive".
- A multi-racial, multi-cultural country like India, where free speech is susceptible to misuse on sensitive grounds of communal, political and religious bias, needs reasonable restrictions to check misuse. Best way to address the concerns is to come with amendments to the scraped section so that it reduces the discretion in the hands of frontline officers.

We need non-legal initiatives by the government, the media, schools, not-for-profit organizations, religious and caste associations and a slew of other groups to further empower users to deploy such strategies to fight abuse and hate speech over the internet.

4. Monitoring social networking sites, phone tapping etc. are an infringement on the privacy, but need of the hour in wake of the recent domestic scenario. Examine.

Approach:

Examine both the pros and cons of such surveillance programs and offer some practical suggestions on how the concerns of groups on both sides of the divide could be addressed.

Answer:

- Given the rising incidences of terrorism and security threats, nations across the world, have been monitoring electronic communications for the purpose of protecting and preserving their sovereignty, integrity and security.
- This has come to be seen as inevitable given the use of technology by criminals, terrorists and organized crime syndicates for anti-national activities.
- India's Central Monitoring System (CMS) and the Prism Program of USA are instances of surveillance programs put in place by countries across the world.
- It has been argued that in the event of a conflict between national interest and individual liberties, it is the former that shall prevail. Also, the Right to Privacy is subject to reasonable restrictions on various grounds.
- The proponents of government surveillance argue that such projects will eventually strengthen the security environment in the country.
- The proponents also argue that while in traditional surveillance systems secrecy could be easily compromised due to manual intervention at various stages, this shall be minimized in new systems like the CMS. This is because in CMS, functions will be performed on a secured electronic link and there will be minimum manual intervention.
- However, the critics express concern over the sheer lack of public information on such projects. There is hardly any official word from the government about which government bodies or agencies will be able to access the data, how they will use this information, what percentage of population will be under surveillance, or how long the data of a citizen will be kept in the record.
- This makes it impossible for citizens to assess whether surveillance is the only, or the best, way in which the stated goal can be achieved. Also, citizens cannot gauge whether these measures are proportionate i.e. they are the most effective means to achieve this aim.
- In such projects, often there is also no legal recourse for a citizen whose personal details are being misused or leaked from the central or regional database.
- Blanket surveillance techniques, like the CMS, also pose a threat to online business. With all the data going in one central pool, a competitor or a cyber criminal rival can easily tap into private and sensitive information by hacking into the server.
- There is also the possibility that as vulnerabilities will be introduced into Internet infrastructure in order to enable surveillance, it will undermine the security of online transactions.
- These projects can also undermine the confidentiality of intellectual property especially pre-grant patents and trade secrets. Rights-holders can never be sure if their IPR is being stolen by some government in order to prop up national players.

- Civil rights groups also argue that security cannot be prioritized by large-scale invasions of privacy, especially in a country like India where there is little accountability or transparency.
- In light of these arguments there is an urgent requirement for a strong legal protection of the right to privacy; for judicial oversight of any surveillance; and for parliamentary or judicial oversight of the agencies, which will do surveillance.
- Moreover, an attempt must be made to reach a middle ground between privacy and security - a system, which takes care of national security aspect and yet gains the confidence of the citizens. The secrecy period can be kept restricted to three to four years in such projects. Thereafter who all were snooped and when and why and under whose direction/circumstances must be made public through a website after this time gap.

5. Assess the potential of Social Media Networks for effective policing in India. Also, highlight the reasons behind relatively slow pace of adaptation of social media into policing in India.

Approach:

- Write down and assess the potential of social media for effective policing.
- Mention the reasons which have led to slow pace of adaptation of social media into policing.

Answer:

The Police departments, globally as well as in India, are increasingly dependent on technology to gather information, create awareness and maintaining a public interface. In this context, social media provides huge potential for policing in India, as millions of Indians are active users of Facebook, Twitter, WhatsApp and other platforms. This can be understood from the following points:

- Problem solving in policing requires information exchange, problem identification, problem solving and trust. Social media can help with all these aspects.
- Social Media can support policing by increasing citizen participation to identify crime, reducing the communication gap and improve co-ordination between the police and citizens. For e.g. timely reporting of criminal activities by citizens helps in prevention and investigation of crime etc.
- Feedback from citizens and understanding their grievances and opinion through social media leads to a holistic development of the police department.
- Some social media tools facilitating anonymity help citizens overcome their social fear to complain about issues of law and order.
- Social media helps in disseminating information and forewarn citizens about areas that might see a conflict. Police uses Facebook and twitter pages to keep citizens informed about policing arrangements.

Nonetheless, these very factors also put certain limitations and challenges for policing:

- Social media has made it possible to spread rumour and create panic in a short span of time.
- It has also made the police personnel, even their personal lives, subject to intense scrutiny. Anonymity makes it easier to make frivoulous allegations tarnishing the image of a police peronnel.
- The widespread use of social media also poses a challenge of gathering actionable intelligence through a vast swathe of data.

Overall the potential utility as well as challenges posed by the widespread use of social media makes it imperative that the police adapts to the changing scenario.

However, adaptation of social media in policing has been very slow. This is due to the following reasons:

- The lack of manpower as well as of technological capabilities of handling social network pages of police inhibits social media adoption for community policing.
- Resistance to technology by police departments in some states
- Digital illiteracy in general and lack of awareness among people regarding use of social media for policing in particular is an inhibiting factor.
- Unclear and generic information from police and violent and abusive content from citizens reduces the efficacy of social media for policing.
- An absence of comprehensive policy in many states regarding use of social media in policing.
- It is very difficult to segregate genuine complains. Thus, there is a chance to misuse social media to spread rumours.
- Concerns regarding data safety and privacy also is becoming a major hurdle in adopting social media in policing

The aim of social media is to achieve decentralized decision-making that empowers field officers to identify crime, prioritizing the problem with the help of local citizens, and introducing transparency in the policing. An efficient social media strategy that focuses on the potential rewards of using social media and mitigating its risks is the need of the hour.

6. Identify the opportunities and challenges that social media presents to the law enforcement agencies in India to counter national security threats. What steps have been taken to address the challenges?

Approach:

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

Answer:

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

Opportunities:

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

Challenges:

- **Increased number of cyber-crimes:** Criminals are using social media for sale of contraband items, selection of targets and victims, spreading malware, committing cyber frauds, impersonation, hacking etc. For example, recently, Pakistan has been found 'honey trapping' Indian soldiers, scientists etc.
- **Unregulated space for propaganda:** Terrorists and extremists are using social media to propagate their ideology and recruit members. For example, radicalisation done by ISIS and use of tremendous online following by Burhan Wani to strengthen Hizbul Mujahideen in Kashmir Valley.
- **Fast paced spread of misinformation:** Foreign entities are using social media as a weapon in their psychological operations to cause unimaginable disruptions. For e.g. Pakistan's ISI uploaded fake inflammatory videos, which triggered exodus of people from North-eastern India staying in Bangalore and Pune.
- **Ineffective laws:** The Indian legal framework that includes IT Act, 2000 and National Cyber Security Policy, 2013 is both inadequate and face limitations in present circumstances. For e.g. denial by WhatsApp to help trace the origin of posts which led to lynching of 5 men in Maharashtra.
- **Democratic rights:** It is also difficult for India to strictly regulate the social media because freedom of speech and privacy are fundamental rights.

Steps taken by India:

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

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

Heartiest Congratulations
to all Successful Candidates

Aditya Srivastava

16 in **TOP 20** Selections in **CSE 2023**
from various programs of **Vision IAS**

Animesh Pradhan

Ruhani

Srishti Dabas

Anmol

Nausheen

Aishwaryam Prajapati

39 Selections in **TOP 50** in **CSE 2022**

Ishita Kishore

Garima Lohia

Uma Harathi N

SHUBHAM KUMAR
CIVIL SERVICES EXAMINATION 2020

DELHI

HEAD OFFICE
Apsara Arcade, 1/8-B 1st Floor, Near Gate-6 Karol Bagh Metro Station

MUKHERJEE NAGAR CENTER
Plot No. 857, Ground Floor, Mukherjee Nagar, Opposite Punjab & Sindh Bank, Mukherjee Nagar

GTB NAGAR CENTER
Classroom & Enquiry Office, above Gate No. 2, GTB Nagar Metro Building, Delhi - 110009

FOR DETAILED ENQUIRY
Please Call:
+91 8468022022,
+91 9019066066

enquiry@visionias.in /c/VisionIASdelhi /visionias.upsc /vision _ias VisionIAS_UPSC

AHMEDABAD BENGALURU BHOPAL CHANDIGARH DELHI GUWAHATI HYDERABAD JAIPUR JODHPUR LUCKNOW PRAYAGRAJ PUNE RANCHI

VISIONIAS
INSPIRING INNOVATION

Classroom Study Material

INTERNAL SECURITY

SECURITY CHALLENGES AND THEIR MANAGEMENT IN BORDER AREAS

CONTENTS

1. Introduction

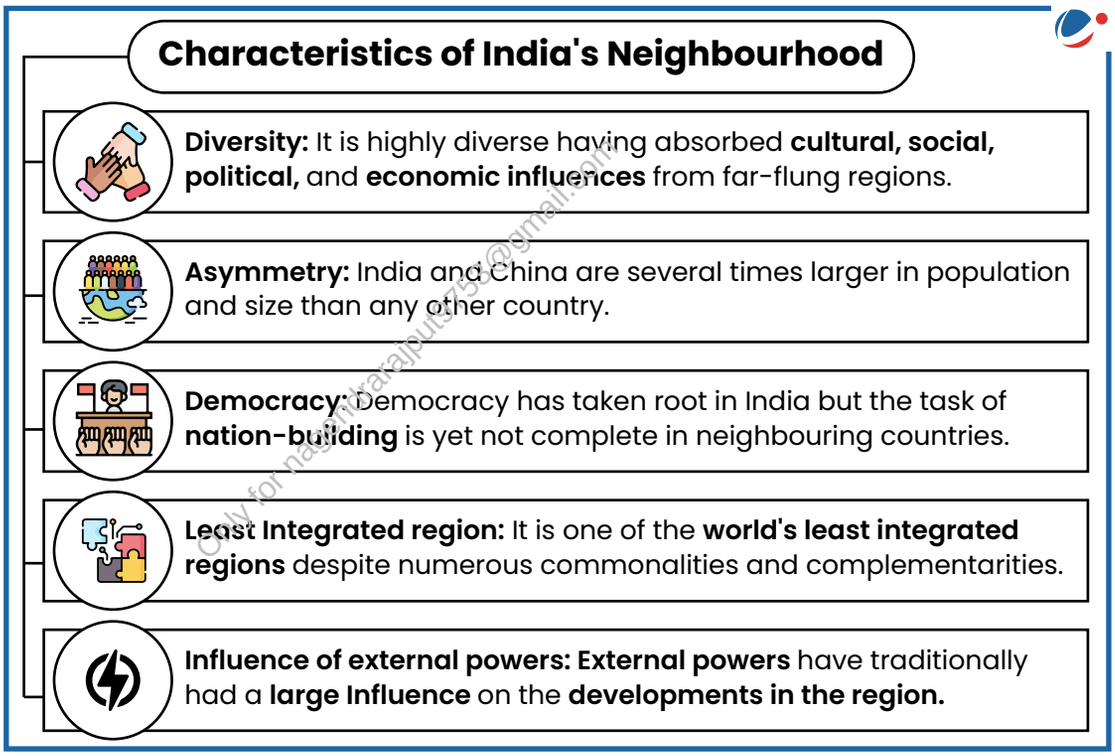
India has 15,106.7 km of land border and a coastline of 7,516.6 km including island territories. Securing the country's borders against interests hostile to the country and putting in place systems that are able to interdict such elements while facilitating legitimate trade and commerce are among the principal objectives of border management. The proper management of borders, which is vitally important for national security, presents many challenges and includes coordination and concerted action by administrative, diplomatic, security, intelligence, legal, regulatory and economic agencies of the country to secure the frontiers and subserve its best interests.

1.1. What is Border Management

While **Border Security Approach** deals only with defending the borders, the **Border management** is a broader term which involves not only defending the borders but also the protection of interests of the country in aligning borders.

The **Department of Border Management** in the Ministry of Home Affairs focuses on management of the international land & coastal borders, strengthening of border policing & guarding, creation of infrastructure such as roads, fencing & flood lighting of the borders and implementation of the Border Area Development Programme (BADP).

Some **problems currently afflicting** the management of our borders including maritime boundaries are:

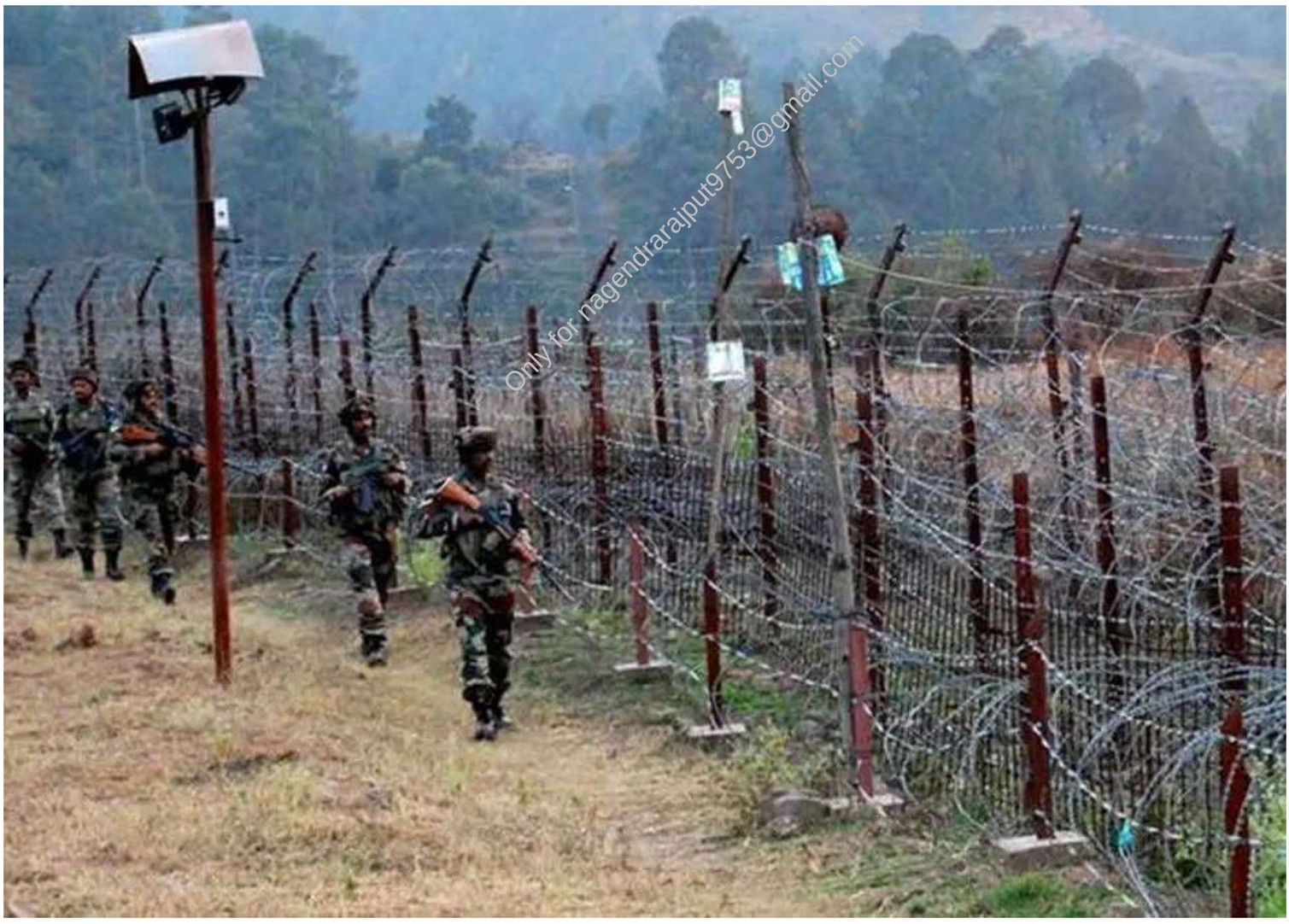


- Hostile elements have access to latest **technology**, unprecedented use of **money power, organisational strength, maneuverability**, wide choice available for **selecting theatre of action** for surprise strikes and **strategic alliances** with other like-minded groups.
- **No proper demarcation of maritime and land borders** at many places leading to conflicts.
- **Artificial boundaries having difficult terrains like deserts, swampy marshes etc. which are not based on natural features** thus making them extremely porous and easy to infiltrate.
- **Multiplicity of forces** on the same borders leading to problems of coordination, command and control. For example, the LAC along China is guarded by Vikas Battalions in some parts of Western and Middle

sector which reports to the Cabinet Secretariat while the ITBP which mans most of the Chinese border is under Ministry of Home Affairs, making coordination difficult.

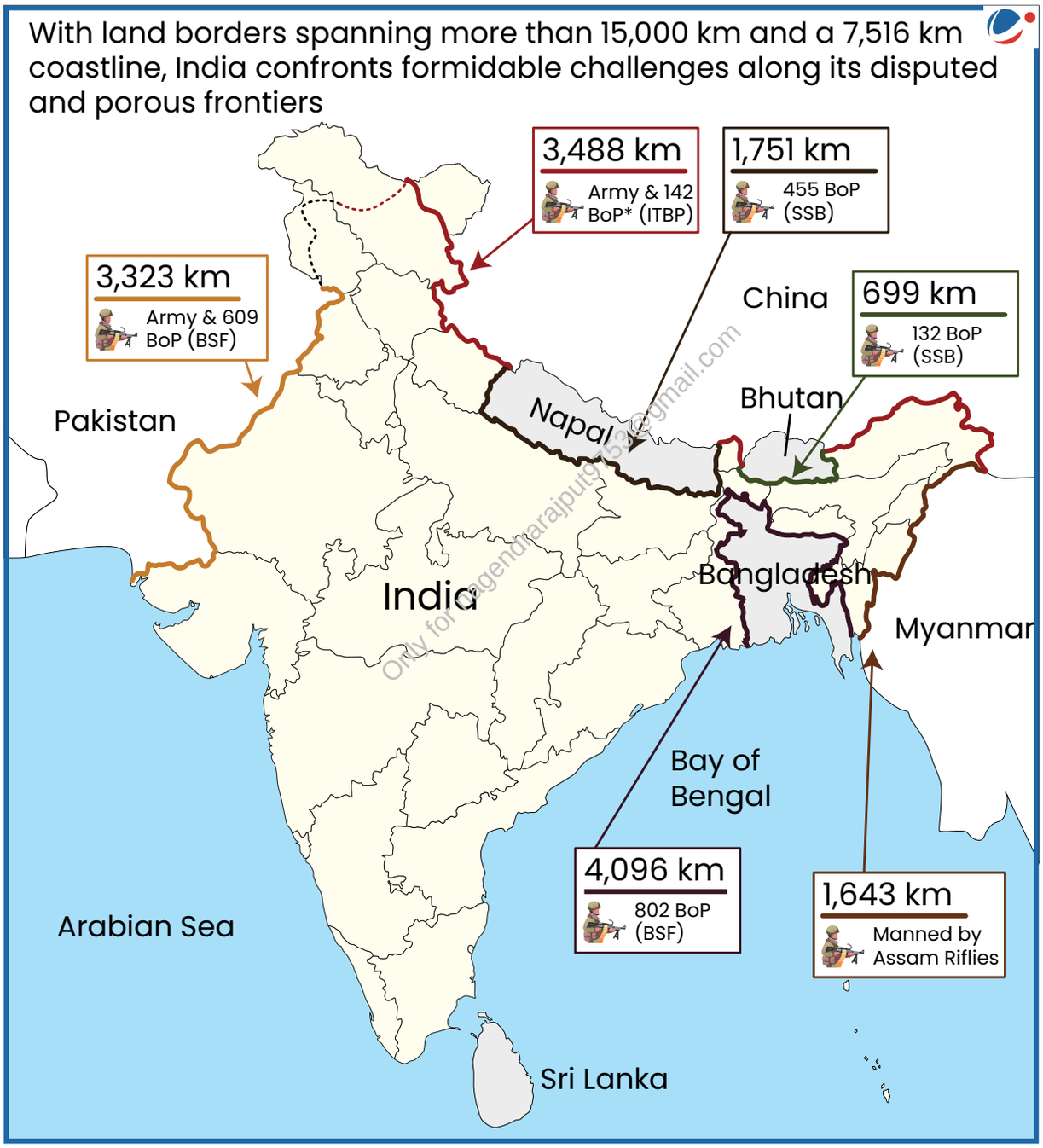
- Border Guarding Forces like Border Security Force etc. **lack infrastructure**. They need to be appropriately strengthened both in terms of equipment and manpower.
- **Problems faced by local people** due to tough measures taken during anti-terrorism and anti-insurgency operations generate discontent which should be addressed prudently otherwise hostile elements try to leverage this discontent to their benefit.
- **Cross-border terrorism** targeted to destabilise India.
- **Illegal migration** in eastern region causing socio-economic stress as well as demographic changes.
- Sporadic aggression on the **border** with China, especially in the Western and Eastern sectors.
- Cross border **safe houses** for insurgent in north eastern neighbours.
- **Smuggling** of arms and explosives, narcotics and counterfeit currency.
- Enhanced instances of **smuggling, piracy, breach of coastal security.**

In light of above stated problems, there is need for utmost vigilance on the borders and strengthening of the border guarding forces. However, it should also be taken care that the security of borders does not impede cross-border interactions and is beneficial to mutual economic and cultural relationship.



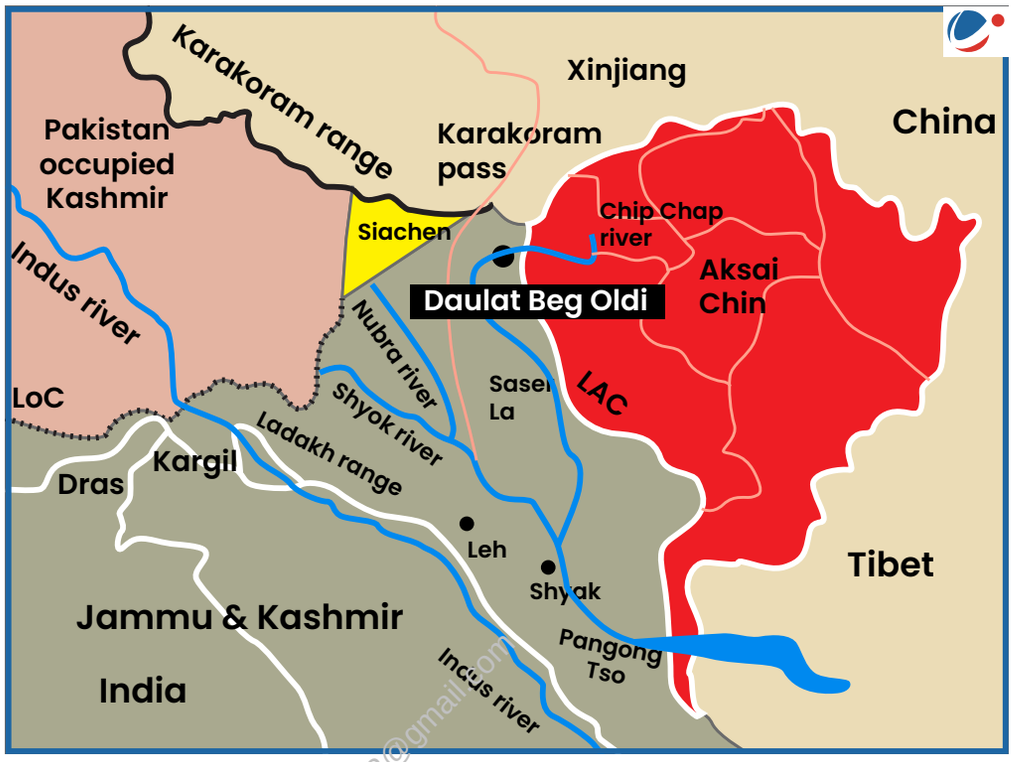
2. Indo-China Border

India and China share a 3,488 km long boundary that runs along the states of Jammu & Kashmir, Himachal Pradesh, Uttarakhand, Sikkim and Arunachal Pradesh. Unfortunately, the entire boundary, called the McMahon line, is disputed. The Indo-Tibetan Border Police Force (ITBP) guards Indo-China border. India and China had never shared a common boundary till China "liberated" or occupied Tibet in 1950. It was then that the hitherto India Tibet boundary was transformed into India-China boundary. Since 1954, China started claiming large tracts of territory along the entire border such as Aksai Chin in Jammu and Kashmir, some areas in Uttarakhand and the entire Arunachal Pradesh.



2.1. Challenges Along the China Border

- **Smuggling:** Large scale smuggling of Chinese electronic and other consumer goods take place through these border points.
- **Inadequate infrastructure:** The area is characterized by high altitude terrain and thick habitation. While China has built massive rail road linkage on its side, Indian side of border was lacking robust infrastructure till recent times.



- **Border Disputes:**
  - **Western Sector - Aksai Chin**

    In 1865, **Johnson line** which put Aksai Chin in Jammu and Kashmir but China at that time did not control Xinjiang so it was not presented to them. By 1890, China re-established control over Xinjiang and claimed Aksai Chin. Then, **Macartney-Macdonald line** was agreed to by the British government on the proposal by Chinese. However, Chinese government did not respond to the note to this effect in 1899 and the British took that as Chinese acquiescence.

    After 1947, India used the **Johnson Line** as the basis for its official boundary but in 1950s China built a road falling south of this line in the Aksai Chin region. Intermittent clashes along the border culminated into Indo-China war in 1962 which resulted into existing line which is known as **Line of Actual Control (LAC)**. The region also witnessed stand-off between India and China in **Daulat Beg Oldie sector in 2013.**

  - **Eastern Sector - Arunachal Pradesh**

    In **Shimla Accord (1913-14),** boundary between Tibet and British India was defined by negotiations between British India, China and Tibet. This boundary named as MacMohan Line is disputed by China. However, interestingly, China accepts MacMohan line as its boundary with Myanmar provided by the same agreement.

  - In the **Middle Sector** (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.

- Indian side of border is being guarded by **different agencies** which include ITBP, Special Frontier Forces, Assam Rifles, Indian Army and proposed Sikkim Scouts leading to **lack of coordination** among these agencies. On the other hand, on the Tibetan side, the entire LAC is managed by Border Guards divisions of the Chinese People's Liberation Army (PLA) under a single PLA commander of the Tibet Autonomous Region.

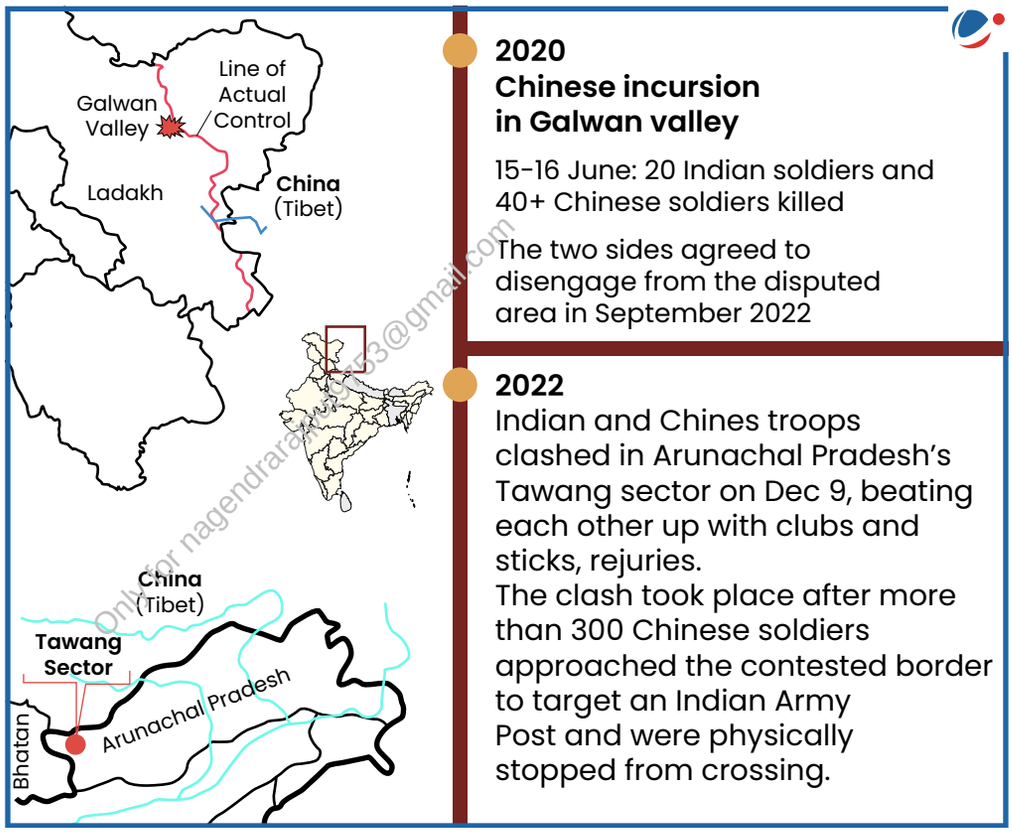
- **China Pakistan Economic Corridor (CPEC):** China's CPEC passes through parts of Jammu & Kashmir illegally occupied by Pakistan. China can use CPEC to mobilize troops in case of conflict and also will provide some cushion against choking of Strait of Malacca by India in case of conflict.
- **Water disputes:** China recently cut off the flow of a tributary of the Brahmaputra River, the lifeline of Bangladesh and northern India, to build a dam as part of a major hydroelectric project in Tibet. And the country is working to dam another Brahmaputra tributary, in order to create a series of artificial lakes. China has also built six mega-dams on the Mekong River, which flows into Southeast Asia, where the downstream impact is already visible. Yet, instead of curbing its dam-building, China is building several more Mekong dams.

2.1.1. Recent Border Tensions between India and China

The most serious recent episodes of conflict between the Indian and the Chinese soldiers were in Galwan Valley in Ladakh in 2020 and in Tawang in **Arunachal Pradesh in 2022.**

The Galwan Valley battle - fought with sticks and clubs, not guns - was the first fatal confrontation between the two sides since 1975.

Another face-off in January 2021 at Naku La in north Sikkim left troops on both sides injured.



Reasons for the these standoffs include:

- **Issues of border demarcation:** The border between India and China is not clearly demarcated throughout and there is no mutually agreed Line of Actual Control (LAC) along certain stretches.
- **Territorial Claims:** Both countries have competing territorial claims in several regions along their border, including the Aksai Chin region in the western sector and the Arunachal Pradesh region in the eastern sector
- **Strategic gains:** Control over border regions provides strategic advantages such as access to natural resources, strategic military positioning, and geopolitical influence.
  - The disputed territories are often rugged and remote, but they hold significant strategic importance for both countries, especially in terms of border security and territorial integrity.
- **Infrastructure build-up,** particularly in Tibet including roads, airstrips, and military installations.
  - This infrastructure development by both countries exacerbates tensions by increasing the presence and capabilities of military forces in disputed areas, heightening the risk of confrontation and escalation.

- **Reorganisation of Jammu and Kashmir:** China had earlier also protested against the formation of new Union Territory of Ladakh and accused India of trying to transform the LAC unilaterally.
- **Growing India-US bonhomie:** In recent few years India has moved closer towards the US. On the other hand, China is engaged in a trade war with US and facing US's opposition over its actions in South China Sea, Hong Kong, and current COVID-19.

In a broader context, the recent confrontations are continuation of the earlier Depsang plains (Ladakh) skirmishes of 2013-14 and the 2017 China-India standoff at Doklam (Bhutan). India's strong opposition had prevented China from extending a track in the contested area at the tri-junction of India- China-Bhutan

2.2. Initiatives Taken for Effective Border Management

- **Border talks:**
  - The rapprochement in 1976 after 1962 war between the two countries led to initiation of High Level border talks in 1981 which broke down in 1987.
  - In 1988, following PM Rajiv Gandhi's visit to China, the Joint Working Group (JWG) was set up to look into border problem. (Refer to the box for series of five Border Dispute Settlement Mechanism)
  - In 2003, two **special representatives** (one each from India and China) were appointed to find a political solution to the border dispute.
  - Till 2009, these two special representatives had held 17 rounds of talks, but it seems they have not made much headway.
  - Recently, NSA Ajit Doval was appointed as Special Envoy for talks.

Unfortunately, despite several rounds of talks, disagreement on actual border continues and both the sides regularly send patrols to LAC as per their perception and leave markers in the form of burjis (piles of stones), biscuit, cigarette packets etc. to lay stake to territory and assert their claim. These patrols often lead to physical confrontation.

- **Construction of roads along India-China border**

In the past decade, India has worked hard to strengthen its position on the border and its presence along the LAC. India is close to completing a major upgrade of border roads, including a strategic military-use road that connects an airfield at Dalut Beg Oldie in the northern tip of the western sector with the

Border Dispute Settlement Mechanism

A series of five agreements signed between India and China to address disputes arising over the LAC:

- **1993 Agreement** on the Maintenance of Peace and Tranquility along the LAC.
- **1996 Agreement on Confidence-Building Measures** in the Military Field along the LAC.
- **2005 Protocol** on Modalities for the Implementation of Confidence-Building Measures in the Military Field along the LAC.
- **2012 Agreement** on the Establishment of a Working Mechanism for Consultation and Coordination on India-China Border Affairs.
- **2013 Border Defense Cooperation Agreement.**

These agreements provide a modus operandi for diplomatic engagement at the military and political levels, as well as a set of "status quo" commitments both sides can return to in case of escalation.

Confidence Building Measures

- Regular interaction between the Army Headquarters and Field Commands of the two sides.
- Additional border personnel meeting points.
- More telecommunication linkages between their forward posts at mutually agreed locations.

villages of Shyok and Darbuk toward the south. Completed in 2019, this "DS-DBO road" greatly facilitates the lateral movement of Indian forces along the western sector, reducing travel time by 40%.

- **Spy Cam Project -** Putting up cameras with 20-25 km range at 50 locations in Himachal Pradesh, Jammu and Kashmir, Sikkim and Tawang in Arunachal Pradesh after 21-day face-off with the People's Liberation Army (PLA) of China at Depsang Valley in the Ladakh region in 2013. But project failed since weather is not favourable there as high-velocity winds and frost tend to blur the images.

2.3. Way Forward

The settlement of the India-China border dispute appears most unlikely in the foreseeable future. So, we should ensure following:

- Our troops should be **battle ready** which could well entail delivering massive artillery fire in a minimal time-span should the security needs at the local level so require
- There should be a well-established **logistics organisation** that can effectively support the existing deployments and any tactical operations that we may need to undertake in the areas.
- The responsibility for the security and surveillance of the IB and the defence of the border zones along the entire length of the India-China border needs to be **transferred to the Ministry of Defence** which should be designated as the 'nodal-agency' and the responsibilities in the field thence be assumed by the army.
- **ITBP**, a force specifically trained for border guarding duties on the India-China border, should not be used by the home Ministry for internal security duties in the naxalite-infested areas of Andhra Pradesh, Chhattisgarh, Jharkhand and Orissa. This **diversion** leads to disturbing the balance and coherence in our deployments.
- **Water Disputes**
  - There is need of improving diplomatic communication, more transparency by way of all-year hydrological sharing of data and exchange of information regarding infrastructural development in the area and developing effective and innovative frameworks of resource management including all stakeholders
  - It also needs to de-emphasize China's role for the time being and re-strengthen its relationship with lower riparian countries including Bangladesh and restore its image as a responsible upper riparian.

3. Indo-Pakistan

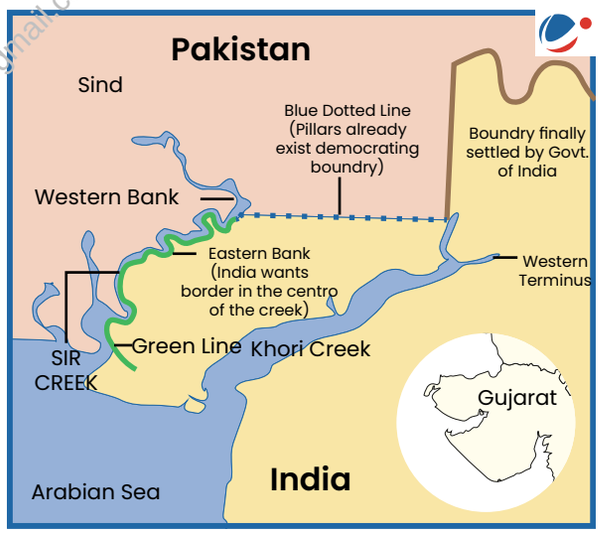
India shares 3323 km long boundary with Pakistan. The border spreads across extreme climatic conditions as the boundary runs from the hot Thar Desert in Rajasthan to the cold Himalayas in Jammu and Kashmir. Thus, the India-Pakistan boundary can be categorized under three different heads.

- **First –** It is 2308 km long and stretches from Gujarat to parts of Jammu district in Jammu and Kashmir. It is known as the **'Radcliff line'.**
- **Second –** It is 776 km long, and runs along the districts of Jammu (some parts), Rajouri, Poonch, Baramula, Kupwara, Kargil and some portions of Leh. It 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.
- **Third –** It is 110 km long and extends from NJ 9842 to Indira Col in the North (Siachin Glacier). It is the **actual ground position line** (AGPL).

3.1. Challenges Along the Border

3.1.1. Sir Creek Dispute

Sir Creek is a 96 km tidal estuary which opens up into the Arabian Sea and divides the Gujarat state of India from the Sindh province of Pakistan. The Sir Creek got its name from the British representative who negotiated the original dispute between the local rulers.



Pakistan's Position

- Pakistan claims the entire Sir Creek, with its eastern bank defined by a **"green line"** and represented on a 1914 map belongs to it.
- Accepting Pakistan's premise on the "green line" would mean loss of about 250 square miles of EEZ for India.

India's Position

- India says that the green line is an indicative line and felt the boundary should be defined by the **"mid-channel"** of the Creek as shown on a map dated 1925.
- India supports its stance by citing the **Thalweg doctrine** in international law. It states that river boundaries between two states may be, if the two states agree, divided by the mid- channel.
- Pakistan maintains that the doctrine is not applicable in this case as it most commonly applies to non-tidal rivers, and Sir Creek is a tidal estuary.

Significance of Sir Creek

- **EEZ –** Accepting Pakistan's premise on the "green line" would mean loss of about 250 square miles of EEZ for India.

- **Energy resource -** Much of the region is rich in oil and gas below the sea bed.
- **Fisherman misery:** The Sir Creek area is also a great fishing destination for hundreds of fishermen from both India and Pakistan.
- **Drug syndicate / Smuggling:** Over the year this region has become main route to smuggle drugs, arms and petroleum product to India.
- **Terror design:** Terrorists are using disputed area to cross over Indian side. In 26/11 terror attack, terrorists captured an Indian fishing vessel, Kuber, off Sir Creek to enter Mumbai.

Timeline of Sir Creek Dispute:

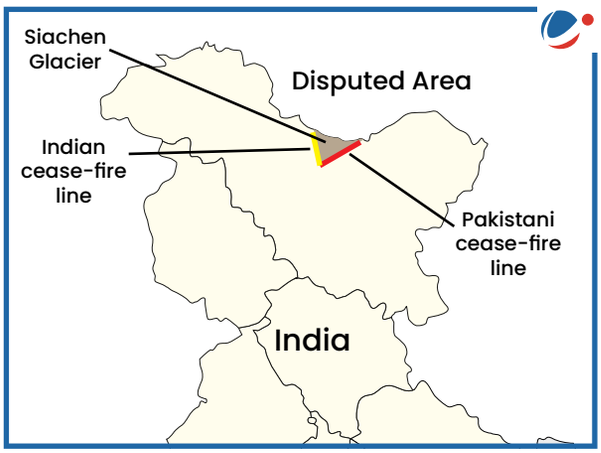
- 1908: Dispute arises between the Rao (ruler) of Kutch and the Sindh government over the collection of firewood from the creek area.
- 1914: The government of Bombay Province took up the resolution and gave award. Paragraph 9 of the 1914 resolution indicates that the boundary in Sir Creek is the green band on the eastern bank of the Creek.
- However, paragraph 10 of the same resolution talks about the centre of the navigable channel being the boundary, incidentally as per the internationally accepted 'Rule of Thalweg'.
- 1925: The land boundary in the horizontal sector was demarcated by Sindh and Kutch in 1924-25 through a placement of 67 pillars.
- 1968: India-Pakistan Tribunal on Kutch border gives its award which upholds 90% of India's claim but it does not cover Sir Creek. The tribunal award relates to the area to the east of sir creek.

Way Forward

- It may be designated as a zone of disengagement or a jointly administered maritime park. Alternatively, given the creek's ecological sensitivity, both countries could designate the area a maritime sensitive zone.
- A transboundary management approach to Sir Creek can address the plight of poor fishermen, who routinely get detained across the border if they drift across the disputed demarcation.

3.1.2. Siachen Dispute

Siachen is a triangular bit of land between Pakistan occupied Kashmir and the part ceded by Pakistan to China.



Reason of Dispute:

- **Ambiguous wording** that exists in the Karanchi ceasefire agreement of 1949 following 1947-48 war.
- The Agreement did not delineate beyond grid reference NJ 9842, which falls south of the Siachen glacier and indicated that the border from NJ9842 runs "thence North to the glaciers".
- Pakistan argues that this means that the line should go from NJ 9842 straight to the Karakoram pass on the Sino-Indian border. India, however, insists that the line should proceed north from NJ 9842 along the Saltoro range to the border with China.

Significance of Siachen

- Siachen sits at a very **strategic location** with Pakistan on the left and China on the right. So Pakistan **re-interpreted the Ceasefire agreement** to claim the area beyond the Saltoro Ridge and beyond Siachen as its own.

- This would give Pakistan **direct connectivity to China** as well as a strategic oversight over the Ladakh region and on to the crucial Leh-Srinagar highway posing a serious threat to India.

Operation Meghdoot

- In 1983, Pakistan tried to use its troops to lay claim to Siachen.
- To pre-empt Pakistan's attempt, India launched **Operation Meghdoot** and occupied the high points of the glacier.
- India currently controls the whole glacier and all three main passes of the Saltoro Ridge namely- Sia La, Bilafond La and Gyond La.

3.1.3. River disputes

- **Kishanganga Hydroelectric Plant**

The Kishanganga Hydroelectric Plant is a run-of-the-river project designed to divert water from the Kishanganga river to a power plant in the Jhelum River basin. In 2010, Pakistan appealed to the Hague's Permanent Court of Arbitration (CoA) against the project under **the Indus Water Treaty.**

The International Court of Arbitration in its "final award" in 2013 allowed India to complete construction of the Kishanganga dam with condition that 9 m3/s of natural flow of water must be maintained in Kishanganga river at all times to maintain the environment downstream.

About Indus Water Treaty -1960

The Indus Waters Treaty is a **water-distribution treaty** between India and Pakistan, brokered by the **World Bank**. The treaty was signed in Karachi on September 19, 1960 by Indian Prime Minister Jawaharlal Nehru and President of Pakistan Ayub Khan. It provided for:

- Control over the three **"eastern"** rivers-the Beas, Ravi and Sutlej-was given to India and the three **"western"** rivers-the Indus, Chenab and Jhelum-to Pakistan.
- Exchange of data and co-operation in matters related to its provisions. For this, it establishes a **Permanent Indus Commission (PIC)** with each country having one commissioner in it.

Review of Indus Water Treaty

In the wake of the **Uri attack,** several experts have demanded that India withdraw from the Indus Waters Treaty whose terms are considered generous to Pakistan. However, officials made it clear that the IWT will hold, at least for the moment. Instead, the Centre drew up a list of measures to optimize use of the Indus waters that India has so far failed to do. Thus, following decisions were taken by the government

- Set-up an inter-ministerial committee to study India's further options.
- Build more run-of-the-river hydropower projects on western rivers, to exploit the full potential of 18,600 MW (current projects come to 11,406 MW).
- Review restarting the Tulbul navigation project that India had suspended after Pakistan's objections in 1987.

Revoking is not the right way forward as it may threaten regional stability and India's credibility globally. Stopping the waters of the Indus rivers can be counterproductive also. India has water-sharing arrangements with other neighbours and not honouring the Indus Treaty would make them uneasy and distrustful. India would lose her voice if China, decides to do something similar.

The IWT turned 60 in September and it is cited as an example of peaceful coexistence that exists despite the troubled relationship between India and Pakistan. The role of India, as a responsible upper riparian abiding by the provisions of the treaty, has been remarkable but the country, of late, is under pressure to rethink the extent to which it can remain committed to the provisions, as its overall political relations with Pakistan becomes intractable.

3.1.4. Gilgit Baltistan Issue

India had opposed Pakistan's order to integrate the region of Gilgit-Baltistan into the federal structure of the country.

In 2018, the executive order from Pakistan's Prime Minister intended to begin legislative, judicial and administrative measures to integrate Gilgit-Baltistan with the rest of the federal structure of Pakistan. This announcement has sparked several protests in the region. In 2020, as per reports, Pakistan has decided to elevate Gilgit-Baltistan's status to that of a full-fledged province.

What is the dispute over Gilgit-Baltistan?

- After the first Indo-Pak war over Kashmir, the UN resolutions created a temporary ceasefire line separating the state into Indian and Pakistani administered regions pending a referendum.
- India, Pakistan and China all claim partial or complete ownership of Kashmir.
  - **India-controlled:** One state, called Jammu and Kashmir, makes up the southern and eastern portions of the region, totaling about 45% of Kashmir.
  - **Pakistan-controlled:** Three areas called Azad Kashmir(AJK), Gilgit and Baltistan make up the northern and western portions of the region, totaling about 35% of Kashmir.
  - **China-controlled:** One area called Aksai Chin in the north-eastern part of the region, equaling 20% of Kashmir.

Significance of Gilgit Baltistan Order

- The order aims to alleviate China's concerns about the unsettled status of Gilgit-Baltistan considering China Pakistan Economic Corridor (CPEC) passes through the disputed region.
- The order has also spread discontent in pro Indian and some other sections of people of Gilgit-Baltistan which want an independent republic in accordance with UN resolutions on Jammu and Kashmir which require Pakistan to withdraw from Gilgit-Baltistan and transfer control to local powers.
- Further such a measure also aims to hide the grave human rights violations, exploitation and denial of freedom to the people residing in Pakistan occupied territories.

- Hitherto Pakistan's federal institutions had maintained that Gilgit-Baltistan is a UN declared disputed area and her residents cannot be declared citizens of Pakistan until India and Pakistan resolve the issue of accession of Jammu and Kashmir.
- India, unlike Pakistan, claims Gilgit-Baltistan as a constitutional part of the country and declares the people of Gilgit-Baltistan as her citizens. In 1994, both houses of the Indian Parliament passed a unanimous resolution reiterating that Pakistani controlled parts of AJK and Gilgit-Baltistan are integral parts of India.

3.1.5. Other issues along the border

- **Cross border firing, border skirmishes and constant tension.**
- **Repeated Infiltration by Pakistan supported terrorists into India as a way of proxy war.**
- **Illegal activities like smuggling, drugs and arm trafficking, infiltration due to porous borders** which runs through diverse terrain including deserts, marshes, plains, snow-clad mountains, and winds its way through villages, houses and agricultural lands.

Challenges faced by border population

- Dearth of jobs
- Lack of proper healthcare services
- Damage to crops in large tracts by waterlogging
- Sometimes border infrastructure violates privacy or hampers their normal life
- Legal and litigation issues of land acquisition while setting up security infrastructure

3.2. Initiatives Taken by Government

- **Fencing -** By 2011, almost all of the border–along J&K, Punjab, Rajasthan and Gujarat – was double-row fenced on the LoC.
- **Use of technology-** The Centre approved a **five-layer elaborate plan** to stop infiltration on the 2,900-km western border with Pakistan.
  - Close Circuit Television cameras, thermal imagers and NVDs, BFSRs, underground monitoring sensors, and laser barriers will be placed along the border to track all movement from the other side.
  - The integrated setup will ensure that in the event of a transgression, if one device fails to work, another will alert the control room.
  - Laser barriers will cover 130 unfenced sections, including riverine and mountain terrain from Jammu and Kashmir to Gujarat, which are often used by infiltrators.
  - The border has been electrified, connected to a range of sensors and strewn with landmines.
  - The entire border is also lit up with strong floodlights installed on more than 50,000 poles. As a result, the Indo-Pak border can actually be seen from space at night.
- **Outposts -** There are about 700 border out posts, one Integrated Check post is there at Attari, Amritsar.
- A program for **Optimal Utilization of Waters of Eastern Rivers of Indus River System** has also been started.

Madhukar Gupta Committee

- It was tasked give recommendations for strengthening border protection and addressing the issue of gaps and vulnerability in border fencing along India-Pakistan Border.
- It was constituted three months after the terror attack on Pathankot IAF base in January 2016 by Jaish-e-Mohammed (JeM) terrorists from Pakistan
- Recommended the use of scientific technology in border management. For example, use of laser fencing, ground sensors and thermal imaging where physical fencing is not feasible due to difficult terrain.
- It gave separate recommendations for four states as each of them has different topography and problems.

Way Forward

- Prompt and **appropriate compensation** to border population to stem dissatisfaction among local people.
- **Study the pattern of illegal activities** like money laundering and checking them.
- The government also established a Task Force on border management under the Chairmanship of **Madhav Godbole**. The report observed that the country's borders could not be effectively managed because of certain **inherent problems** such as their disputed status, artificiality, porosity etc. which give rise to multiple other problems including illegal migration, smuggling, drugs trafficking, and trans-border movement of insurgents.

Its recommendations are:

- Pending border disputes with neighbouring countries should be resolved.
- The border-guarding force **should not be deployed for other internal security duties.**
- A **Marine police force** should be established along with the strengthening of the Indian Coast Guard and setting up of an apex institution for coordinating various maritime issues.
- Accelerated **development of infrastructure** along the border should be taken up, especially to wean the border population from illegal activities.

4. Indo-Nepal

As per MHA, India shares a 1751 Km long border with Nepal. Uttarakhand, Uttar Pradesh, Bihar, West Bengal and Sikkim are the states, which share the border with Nepal. Bihar shares the largest border and Sikkim the smallest with Nepal.

The border with Nepal is an **open border** and was virtually unattended till very recently as Nepalese citizens have free access to live and working India under a **1950 treaty** between the two countries. Nepal is a **landlocked country** and its closest access to the sea is through India. As a result, most of its imports pass through India. Keeping this in consideration, India has granted Nepal 15 transit and 22 trading points along the border.

4.1. Challenges Along the Border

- **Pakistan is using the open borders to carry out anti-India activities including pushing of terrorists and fake Indian currency.**
- **Fear of spread of Maoist insurgency** and links with Maoists groups in India
- **Issue of land grabbing -** Allegations of excesses such as intimidation, and forcible grabbing of land by either side along the disputed border also surface from time to time.
- **Easy escape & illegal activities -** Insurgents, terrorists, many hard-core criminals pursued by Indian and Nepalese security forces escape across the open border.

4.1.1. Recent Border Dispute

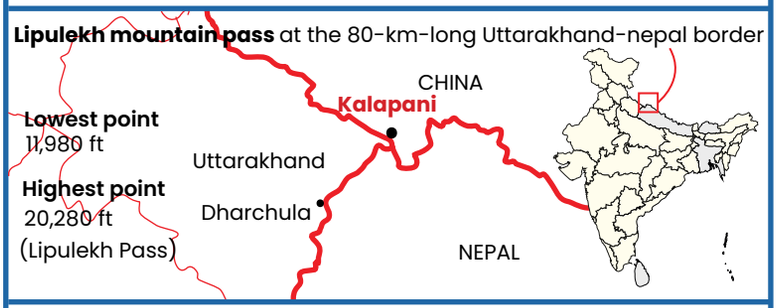
Recently, Nepal unveiled a new political map that claimed strategically important land **Kalapani, Limpiyadhura and Lipulekh** of Uttarakhand as part of its sovereign territory. Nepal considers the 1816 **Treaty of Sugauli** (signed between Gurkha rulers of Kathmandu and the East India Company) as the only authentic document on boundary delineation.

- Under the provisions of the Sugauli Treaty, Nepal lost Sikkim, Kumaon, Garhwal and Western Terai (Flat) area. River Mechi became the eastern border with India while the river Kali (called Mahakali in Nepal) was demarcated as the north-western border. The Treaty of Sagauli also defined Gandak as the international boundary between India and Nepal.
- Nepal considers the source of Kali river near Limpiyadhura, which is higher in altitude than the rest of the river's flow. Thus, all the three areas Limpiyadhura, Lipulekh and Kalapani are considered to the east of the river Kali.

India on the other hand says the border begins at Kalapani which India says is where the river begins.

- Kali originates in springs well below the Lipulekh pass, and the Sugauli treaty does not demarcate the area north of these streams.
- Administrative and revenue records going back to the nineteenth century show that Kalapani was on the Indian side, and counted as part of Pithoragarh district, now in Uttarakhand.
- India has controlled this territory since 1950s and built other infrastructure here before, besides conducting its administration and deploying military forces up to the border pass with China.
- China in 2015 statement also recognised India's sovereignty over the area by agreeing to expand trade through the Lipulekh pass.

Tri-Junction Trouble



- Nepal has two tri-junctions with India and China
- The one in dispute now is Lipulekh in Kalapani, at the border of Uttarakhand with Nepal
- In 1816, the Sugauli Treaty signed by Nepal and British India identified Kali river as Nepal's boundary with India
- Nepal claims the river to Kalapani's west is the main Kali, and thus Nepal has territorial rights to it
- India holds that a ridgeline to Kalapani's east is the border, thus Kalapani falls within its territory

4.2. Initiatives Taken for Effective Border Management

- 25 batallions of **Shashastra Seema Bal under Ministry of Home Affairs** have been **deployed**.
- **Bilateral talks -** Bilateral mechanisms in the form of **Home Secretary-level talks and Joint Working Group** at the level of Joint Secretaries exist between the two countries.
- **Border District Coordination Committee -** At the level of district officials of the two countries- has been established as platforms for discussing issues of mutual concern.
- **Construction of Indo-Nepal border roads -** The Government of India has approved construction of 1377 km of roads along Nepal border in the States of Uttarakhand, Uttar Pradesh & Bihar.

4.3. Way Forward

- Security agencies of both countries should **coordinate** more closely and effectively for better monitoring of the border. An increased use of technology in monitoring border movement can also help to secure the open border.
- A **Joint Boundary Demarcation Committee** could be appointed by both the countries to scientifically study the Maps and come to a conclusion diplomatically.

5. Indo-Bhutan

Indo-Bhutan border is demarcated except along the tri-junction with China. The process of demarcation of the India-Bhutan border started in 1961 and was completed in 2006. This border is defined by foothills, unlike the complex topography of dense forests, rivers and populations that defines India's borders with Nepal and Bangladesh.

India has a **Friendship treaty with Bhutan** which was re-negotiated in 2007 under which India has a huge stake in safeguarding interests of Bhutan.

The two countries share warm bilateral ties and strong border coordination. For Bhutan, issues of **hydropower and trade** within the region impinge on its border cooperation. Other issues such as rupee trade and banking facilities on both sides of the border are also important.

5.1. Challenges Along the Border

5.1.1. Border Dispute

The border is not demarcated in tri-junction area. Thus, the conflict arises such as recent Doklam issue.

5.1.1.1. Doklam Issue

Doklam plateau is a part of Bhutan disputed by China which can provide China leverage to choke India's **"Chicken Neck"** - the narrow Siliguri corridor which links the north-east with the rest of India. In 2017, India successfully deployed its troops to counter Chinese design to build a road in Doklam which could have serious implication for India's security and would have also signaled to Bhutan that India can no longer protect its interests. So, Indian troops intervened to block the path of Chinese People's Liberation Army soldiers engaged in building road-works on this plateau. **This is the first time that India used troops to protect Bhutan's territorial interests.**

5.1.2. Other Issues

- **'Operation All Clear'** by Royal Bhutanese Army drove out the Bodo and ULFA insurgents from its territory some years ago. The border has been relatively quiet. But still fears are persistent about criminal and militant activity.
- **Smuggling -** Chinese made goods, Bhutanese cannabis, liquor and forest products are major items smuggled into India. Livestock, grocery items and fruits are smuggled out of India to Bhutan.

- **Free movement of people & vehicles –** Bhutan wants free movement of its citizens and vehicles once they enter Indian territory. During the Gorkhaland movement in West Bengal vehicles belonging to Bhutanese nationals were destroyed. From internal security perspective, illicit establishment of camps by militant outfits in the dense jungles of south-east Bhutan is a cause of concern for both the nations.
- **Migration –** As areas bordering Bhutan are largely underdeveloped, many Indians work as manual labour in construction sites in that country, where they manage to earn more decent wages. This migration has provoked concerns of altering demographies in both countries.
- **Environmental concerns -** Migrants and infiltrators are also accused of deforestation, poaching, and wildlife smuggling.

5.2. Initiatives Taken

- **Deployment of forces -** Sashastra Seema Bal **(SSB)** is the main boarder guarding force with some help from BSF.
- **Bilateral cooperation -** A Secretary level bilateral mechanism in the shape of an **India-Bhutan Group on Border Management and Security** is in existence. This mechanism has proved to be very useful in assessing threat perception of the two countries from groups attempting to take advantage of this open border and in discussing ways of improving the security environment in border areas.
- There is also a **Border District Coordination Meeting (BDCM) Mechanism** between the bordering States and the Royal Government of Bhutan (RGoB) to facilitate coordination on border management and other related matters.
- **Road construction -** The Government of India has approved construction of 313 km. road in Assam along Indo-Bhutan border. About 60,000 Indian nationals live in Bhutan, employed mostly in the hydro-electric power construction and road industry.
- The Union environment ministry has given a **"general approval"** for the diversion of forest land for major border infrastructure projects along the eastern border with Bhutan, Myanmar and Nepal.

6. Indo-Bangladesh

The Indian side of the Indo-Bangladesh border passes **through 5 Indian states-** West Bengal, Assam, Meghalaya, Tripura and Mizoram. The entire stretch consists of plains, riverine belts, hills and jungles. The area is heavily populated and is cultivated right upto the border. India and Bangladesh share 54 trans-boundary rivers.

India and Bangladesh have been able to solve some contentious issues through negotiations which experts consider as the **best example of border management such as:**

- India and Bangladesh successfully resolved issue of enclaves through mutual agreement and India enacting **100th Constitutional Amendment Act to this effect.**
- Sharing of Ganga water through a **1996 Agreement** between the two countries. However, Bangladesh has expressed concerns over **Farakka Barrage** which diverts water to the Hooghly river claiming that it does not get a fair share in dry season and gets flooded when India releases water.
- **Maritime disputes:** In 2009, Bangladesh instituted arbitral proceedings for the delimitation of the maritime boundary with India under UNCLOS, the verdict of which settled the dispute in 2014.

Outstanding Issues between the two neighbours:

- **Teesta River Water Dispute:** Teesta River originates from the Pahunri (or Teesta Kangse) glacier in Sikkim, flows through the northern parts of West Bengal before entering Bangladesh. It merges with the Brahmaputra River (or Jamuna in Bangladesh). The river is a major source of irrigation to the paddy growing greater Rangpur region of Bangladesh.
  - In 1983, an ad hoc arrangement on sharing water was made, according to which Bangladesh got 36% and India 39% of the waters, while the remaining 25% remained unallocated. The transient agreement could not be implemented.
  - Bangladesh has sought an equitable distribution of Teesta waters, on the lines of Ganga Water Treaty of 1996.
  - In 2011 India and Bangladesh finalized an arrangement, by which India would get 42.5% and Bangladesh 37.5% while remaining 20% would flow unhindered in order to maintain a minimum water flow of the river. This agreement was not signed due to opposition from chief minister of West Bengal.
- **Tipaimukh Hydro-Electric Power Project** on the **Barak River**- Bangladesh is opposing the project as it says that the dam will disrupt the seasonal rhythm of the river and have an adverse effect on downstream agriculture, fisheries and ecology of the region. Indian government has assured Bangladesh that it will **not take any unilateral decision** on the Project which may adversely affect Bangladesh.
- Due to high degree of **porosity** of Indo-Bangladesh Border, millions of Bangladeshi immigrant mostly illegal have poured into India.
- **Border fencing issue -** There have been some problems in construction of fencing in certain stretches on this border due to:
  - Riverine/ low-lying areas,
  - Population residing within 150 yards of the border,
  - Pending land acquisition cases and
  - Protests by border population, which has led to delay in completion of the project.

- **Unauthorised cross-border trade in goods** such as jamdani sarees, rice, salt and diesel has flourished, despite the presence of strict trade regulations and barriers. Although India and Bangladesh officially trade goods worth $7 billion, illegal trade between the two countries is estimated to be double the figure.
- **Cattle smuggling and killing of smugglers -** Cattle confiscated on border alone are around **one lakh annually** thus a loss of revenue of around 10000 crore annually for the government. A large number of Bangladeshi nationals who are caught smuggling cattle across the border are killed. While the number of recorded deaths has **reduced significantly** after India introduced a **new policy** of having only non-lethal weapons for BSF's use, the measure has emboldened criminals and led to an increase in attacks on BSF personnel.
- **Increasing radicalisation:** Presence of groups like Harkat-al-Jihad-al-Islami (HUJI) and Jamaat-e-Islami fuel Anti-India sentiments in Bangladesh. Their propaganda could spill across border.

Comprehensive Integrated Border Management System (CIBMS)

- The CIBMS is a robust and integrated system that is capable of addressing the gaps in the present system of border security by seamlessly integrating human resources, weapons, and high-tech surveillance equipment along India's International borders with Pakistan and Bangladesh.
- CIBMS is being implemented since 2016, after the Pathankot terrorist attack.
- The purpose of the CIBMS is to eventually replace manual surveillance/patrolling of the international borders by electronic surveillance to enhance detection and interception capabilities.
- CIBMS has three components which are using a number of different devices for surveillance, efficient and dedicated communication network and data storage for a composite picture. Sensors like Thermal Imager, Unattended Ground Sensor(UGS), Fiber Optical Sensors, Radar, Sonar, satellite imagery are used in CIBMS.

6.1. Initiatives Taken

- **Deployment of force –** The BSF and BGB have also been raising awareness among the locals regarding crime prevention in the border area.
- In January 2018, Information and Technology Wing of BSF undertook the project **BOLD-QIT (Border Electronically Dominated QRT Interception Technique)** to install technical systems which enable BSF to equip Indo-Bangla borders with different kind of sensors in the unfenced riverine area of the Brahmaputra and its tributaries.
- Government has announced the establishment of **Border Protection Grid (BPG)** with Indo- Bangladesh Border States.
- A crime-free stretch has been established between the BSF border posts at Gunarmath and Kalyani and the BGB (Border Guards Bangladesh) border posts at Putkhali and Daulatpur.
- **Fencing -** India has constructed a barbed-wire fence and improved lighting along the border to prevent illegal immigrant and other anti-national activities.

Drone Technology for Defense in India

LAKSHYA and NISHANT: Unmanned Aerial Systems developed by DRDO.

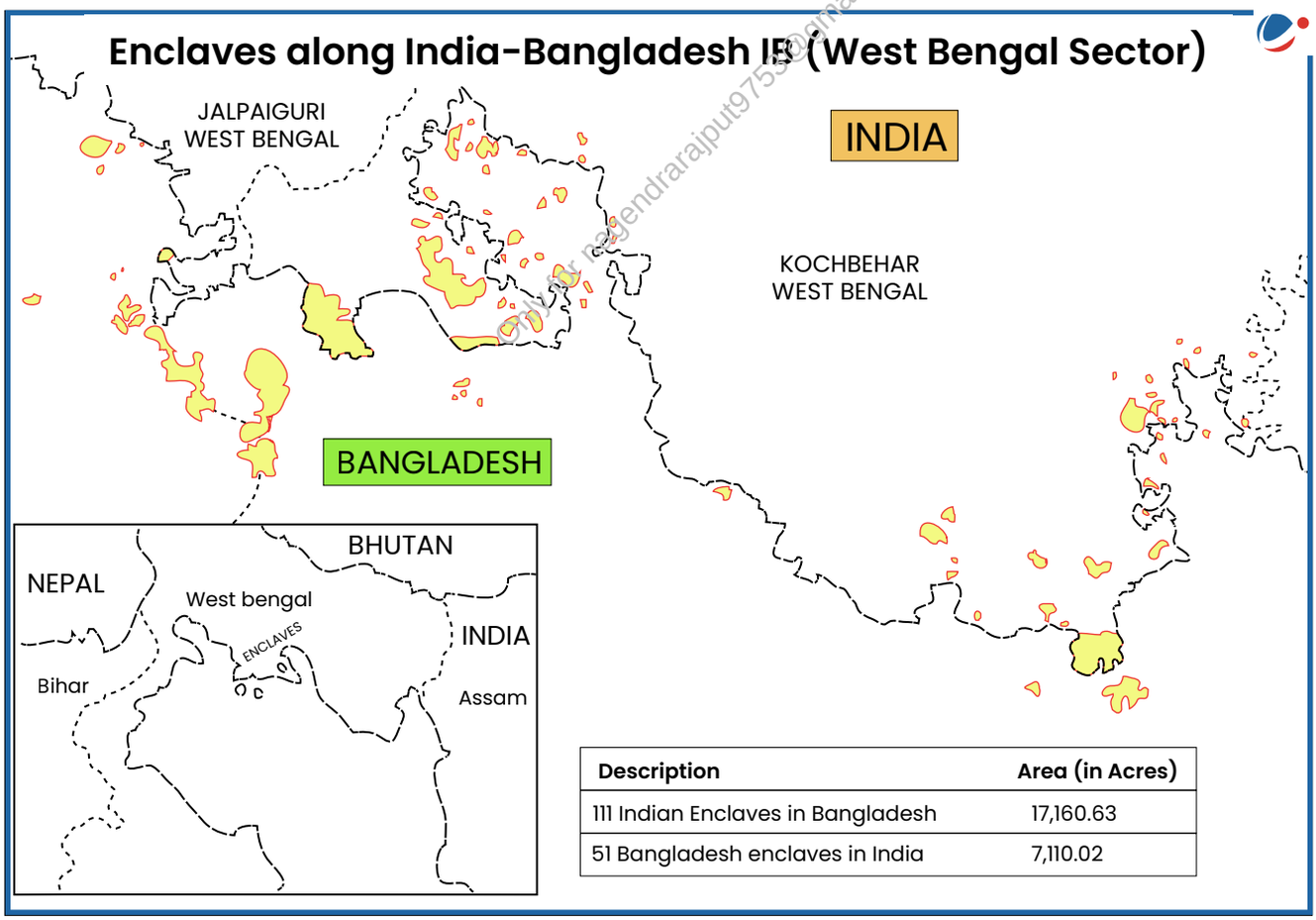
Black Kite, Golden Hawk, and Pushpak: Micro & Mini UAVs developed by DRDO.

DRDO NETRA: Light-weight, autonomous UAV for surveillance and reconnaissance operations.

DRDO Rustom: Medium Altitude Long Endurance UAV developed for Armed forces.

Counter-drone system: Developed by DRDO.

- **Road construction -** In addition, 3,585.53 km of border patrol roads have been constructed out of a sanctioned length of 4,407.11 km. A border management department has also been setup **to oversee developmental work** in the bordering areas and upgraded infrastructure at major entry and exit points.
- **Strengthening vigilance and regulation -** Steps have been taken to strengthen border vigil through enhancement of border guards. India is also **establishing integrated check posts (ICP)** at its land borders which will house, under one roof all regulatory activities such as immigration, security and customs. For e.g. Sutarkandi in Assam, Ghojadanga in West Bengal- integrated check posts along Bangladesh border.
- Installation of **Border surveillance devices** such as closed-circuit cameras, searchlights, thermal imaging devices and **drones** to keep a tight vigil.
- **Bilateral cooperation -** India and Bangladesh have both signed a border management plan that envisions **joint patrols and information-sharing.** India and Bangladesh have also established **border haats** to deal with illegal or unauthorised trade. Two MoUs - one on **Bilateral Cooperation for Prevention of Human Trafficking, Smuggling and Circulation of Fake Currency Notes** and second on cooperation between the **Coast Guards of India and Bangladesh:** to **prevent crimes at sea –** have been signed. Border forces of two countries also undertake joint exercise such as **Sundarban Moitry (Sundarbans Alliance).**
- **Land Boundary Agreement, 2015:** The 2015 LBA implements the unresolved issues stemming from the un-demarcated land boundary—approximately 6.1-km long—in three sectors, viz. Daikhata-56 (West Bengal), Muhuri River–Belonia (Tripura) and Lathitila–Dumabari (Assam); exchange of enclaves; and adverse possessions, which were first addressed in the 2011 Protocol. It is important to note that in the land swap, Bangladesh gained more territory than India did.



Description	Area (in Acres)
111 Indian Enclaves in Bangladesh	17,160.63
51 Bangladesh enclaves in India	7,110.02

7. Indo-Myanmar

India shares 1,643 km long border with Myanmar. Arunachal Pradesh, Nagaland, Manipur and Mizoram are the four States, which share the border with Myanmar. India and Myanmar used to permit a Free **Movement Regime (FMR),** formalized in 2018 as part of India's Act East Policy, for tribes residing along the border to travel upto 16 km across the border. But FMR has been **scrapped in 2024.**

FMR regime conceptualized due to following reasons-

- **Strong ethnic and familial ties across the border:** The border demarcated by the British in 1826 effectively divided people of the same ethnicity and culture into two nations without their consent.
- **Local trade and business:** The region has a long history of trans-border commerce through customs and border haats. Given the low-income economy, such exchanges were vital for the sustenance of local livelihoods.

Reasons for scrapping Free Movement Regime

- **Illegal immigration:** Uncontrolled immigration of Chin people from Myanmar leading to demographic changes in the region
- **Ethnic violence and insurgency:** Meitei community attributed 2023 Manipur tensions to the perceived illegal migration of tribal Kuki-Chin communities.
- **Entry of soldiers from Myanmar:** Exodus of junta soldiers seeking sanctuary in Mizoram which has serious security implications in India's northeast.
- **Surge in narcotics production in Myanmar:** A report by UN Office on Drugs and Crime (UNODC) linked Myanmar's political turmoil under military junta to surge in flow of narcotics in the region

7.1. Challenges at Indo-Myanmar border

Though the boundary is properly demarcated, there are a few pockets that are disputed. The major issues along the border are as follows:

- **Rugged terrain –** It makes movement and the overall development of the area difficult.
- **Weak vigilance -** There is lack of **physical barrier** along the border either in the form of fences or border outposts and roads to ensure strict vigil.
- **Insurgency -** Insurgents make use of the **poorly guarded border** and flee across when pursued by Indian security forces. Close ethnic ties among the tribes such as Nagas, Kukis, Chin, etc., who live astride the border help these insurgents in finding safe haven in Myanmar. These **cross-border ethnic ties** have facilitated in creation of safe havens for various northeast insurgent groups in Myanmar.
- **Drugs menace -** The location of the boundary at the edge of the **"Drugs golden triangle"** facilitates the unrestricted illegal flows of drugs into Indian territory. Heroin is the main item of drug trafficking. The bulk of heroin enters India through the border town of Moreh in Manipur. It is reported that the local insurgent groups are actively involved in drugs and arms trafficking. Smuggling of **ephedrine** and **pseudo-ephedrine and trafficking of women and children** from the Northeast to Myanmar and further to Southeast Asia are also rampant along the border.
- **Boundary dispute -** Even though the international boundary between the two countries had been formally delimited and demarcated following the 1967 Boundary agreement, the boundary has not crystallised on the ground as lines separating two sovereign countries.

- **Lack of attention -** The policymakers in Delhi have not given adequate attention to the India-Myanmar border and as a result it continues to be poorly managed.
- **Lack of support from military Junta Govt. in Myanmar:** India's patchy engagement with the military junta in Myanmar and its initial support to the democratic movement in that country have been largely responsible for Myanmar's reluctance to cooperate with India.

7.2. Steps taken by government

- **Deployment of force –** Assam Rifles mans this border since 2002 with some help from Indian Army. However, Assam Rifles has deployed 31 of its 46 battalions for counter insurgency operations and only 15 battalions for guarding the border thus functioning more like a counter insurgency force rather than a border guarding force.
- **Scrapping free movement regime –** The decision was taken by the central government in 2024 in view of the continued Manipur violence and to stop insurgents like NSCN-K from misusing FMR for receiving training in arms, establish safe havens and re-enter India to carry out subversive attacks.
- Cabinet recently proposed to set up **13 new Integrated Check Posts (ICPs)** to encourage India's engagement with SAARC countries along with Thailand and Myanmar. ICP is able to interdict such elements while facilitating legitimate trade and commerce.

7.3. Way Ahead

Given that the vulnerability of the India-Myanmar border is posing a serious challenge to the internal security of the country, the Government of India should pay immediate attention to effectively manage this border.

- It should first strengthen the security of the border by either **giving the Assam Rifles the single mandate** of guarding the border or deploying another border guarding force such as the Border Security Force (BSF).
- The **construction of the ICP** along with other infrastructure should be expedited.
- Finally, India should endeavour to meaningfully engage with Myanmar and solicit its cooperation in resolving all outstanding issues and better manage their mutual border.

8. Indo-Sri Lanka

Sri Lanka shares maritime border with India and is a very important country strategically placed in Indian ocean for India's security.

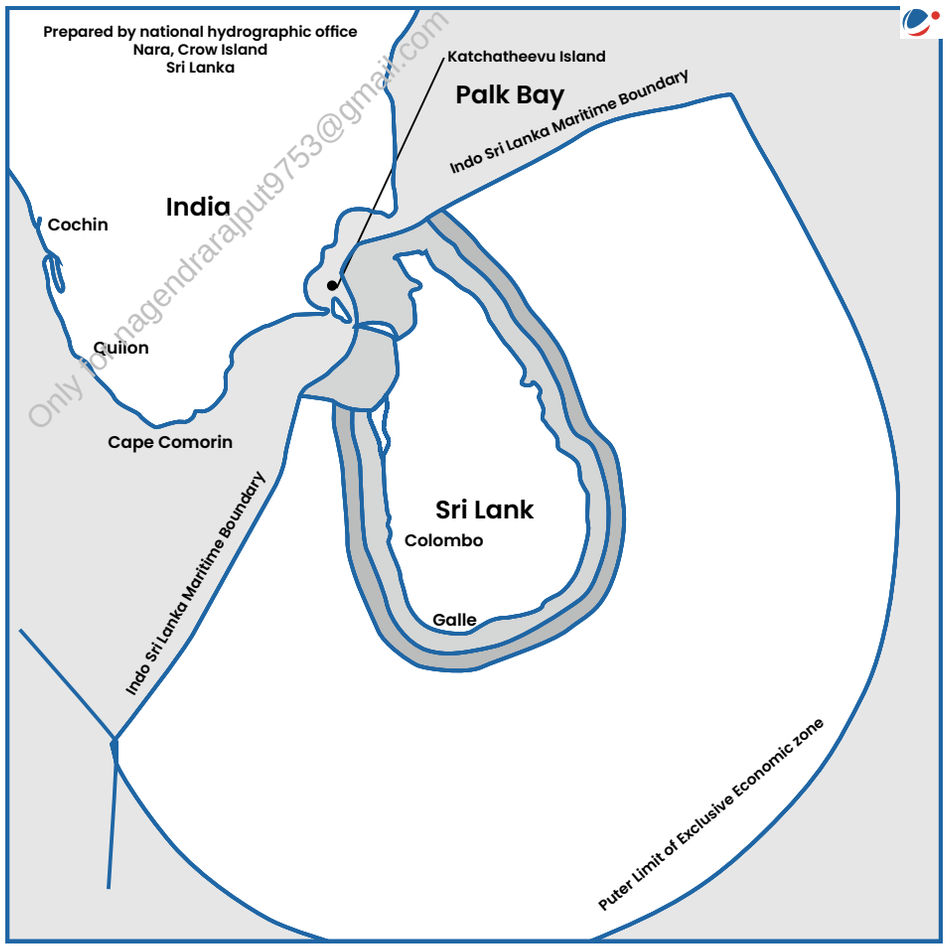
8.1. Challenges along the border

8.1.1. Katchatheevu Island

India ceded the uninhabited island to its southern neighbour in 1974 under a **conditional accord**. However, Indian fishermen considered it to be their traditional fishing area and want Katchatheevu to be used as fishing grounds for India as well.

8.1.2. Fishermen Issue

Trespassing by Indian fisher men in Sri Lankan waters takes place regularly. Here, the issue is not of an **unsettled maritime boundary** but the refusal of Indian fisher men to recognise the maritime boundary between India and Sri Lanka, especially in the **Palk Bay**. The Palk Bay has traditionally been a common fishing ground for fishermen on both the sides. However, the **delineation of the maritime boundary** has divided the Palk Bay, and stipulates that Indian fishermen cannot fish beyond the international boundary. In recent years, Sri Lanka has introduced tougher laws banning bottom-trawling and put heavy fines for trespassing foreign vessels.



Fishing in each other's waters by the fishermen of India and Sri Lanka has strained bilateral ties. Every time an Indian fisherman is arrested by Sri Lankan authorities, Tamil Nadu puts pressure on the Indian government to lodge a formal protest with the Sri Lankan government.

8.2. Initiatives Taken

Regarding fishermen issue

- Steps have been taken to ensure the safety of fishermen, and to prevent the undetected entry of any fishing trawler in the coastal waters. For this purpose, all big fishing trawlers (20 meters and above) are being installed with AIS transponders. As for small fishing vessels, a proposal to fit them with the Radio Frequency Identification Device (RFID) is under consideration.
- Besides, all fishing vessels are also being registered under a **uniform registration system,** and the data is being updated online. **Colour codes** are being assigned to them for easy identification at sea. The colour codes are different for different coastal states.
- Furthermore, **Distress Alert Transmitters** (DATs) are being provided to fisher men so that they can alert the ICG if they are in distress at sea. For the safety of fishermen at sea, the government has implemented a scheme of providing a subsidised kit to the fisher men which includes a Global Positioning System (GPS), communication equipment, echo-sounder and a search and rescue beacon.
- **Coastal security helpline numbers** 1554 (ICG) and 1093 (Marine Police) have also been operationalized for fishermen to communicate any information to these agencies.

8.3. Way Forward

The following steps can be considered to resolve the disputes and challenges between the two countries:

- **Sustainable fishing and alternate livelihood –** There is a glaring need for institutionalisation of fishing in Indian waters by the government of India so that alternative means of livelihood are provided. Government will have to mark up a **comprehensive plan** to reduce the dependence of Indian fishermen on catch from Palk Bay and the use of bottom trawlers from Tamil Nadu, India. Through incentives and persuasion, fishermen from the Palk Bay could be encouraged to switch over to deep-sea fishing in the Indian exclusive economic zone and in international waters.
- **Institutional mechanism –** Last year, the two countries agreed on establishing a Joint Working Group (JWG) on fisheries to help resolve the dispute, setting up a hotline between the Coast Guards of India and Sri Lanka, convening of the JWG once in three months, and meetings of the fisheries ministers every half-year were the components of the mechanism to be put in place.
- **Indian Navy or Coast Guard** should join the **Sri Lankan Navy** in jointly patrolling the international boundary to prevent trespassing.

9. General Recommendations for Better Border Management

Despite several para-military forces guarding borders, the army's commitment for border management amounts to six divisions along the LAC, the LoC and the Actual Ground Position Line (AGPL) in J&K and five divisions along the LAC and the Myanmar border in the eastern sector. This is a **massive commitment** that is costly in terms of manpower as well as funds. According to the availability of funds for modernization, the following steps may be considered:

- **Use of advanced technology** for surveillance particularly satellite and aerial imagery, can help to maintain a constant vigil along the LAC and make it possible to reduce physical deployment.
- **Aerial surveillance** through a **larger number of helicopter units** will enhance the quality and the ability to move troops to quickly occupy defensive positions when it becomes necessary.

Other general recommendations for border management are:

- The **BSF** should be responsible for all settled borders while 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.
- **Effective control -** The principle **of 'single point control' or one-force-one-border principle** must be followed.
- There should be **comprehensive long term planning** for deployment of central police organizations (CPOs) which is currently characterized by **ad-hoc decisions** and **knee-jerk reactions** to emerging threats and challenges. Security strategies should be designed for **'fire prevention' or proactive approach** rather than 'firefighting' approach.
- **Enhancing operational effectiveness** by making all para-military forces managing unsettled borders operate directly under the control of the army.
- **Developing Infrastructure -** Accelerated development of infrastructure along the border, especially to wean the border population from illegal activities.
- **Use of advanced technology -** The advances in surveillance technology, particularly satellite and aerial imagery, can help to maintain a constant vigil along the LAC and make it possible to reduce physical deployment.
- **Up-gradation of intelligence network** and co-ordination with sister agencies, conduct of special operations along the border.
- **Raising the issues of infiltration** from across the border during various meeting with counterpart countries.

10. Government Initiatives for Border Management

10.1. Border Area Development Programme

The Department of Border Management, Ministry of Home Affairs has been implementing a Border Area Development Programme (BADP) through the State Governments as part of a comprehensive approach to Border Management. Its aim is **to meet the special developmental needs** of the people living in remote and inaccessible areas situated near the international border and to saturate the border areas with essential infrastructure through convergence of **Central/State/BADP/Local schemes** and **participatory approach** and to promote a sense of security and well-being among the border population.

- BADP covers all the villages which are located within the **0-10 Km** of the International Border.
- Funds are provided to the States as a **non-lapsable Special Central Assistance** (SCA) for execution of projects relating to infrastructure, livelihood, education, health, agriculture and allied sectors.
  - BADP covers specific planned socioeconomic and infrastructure development in areas such as: Road connectivity, Water and Power supply, Social Infrastructure including Health & Education, Sports activities, Agriculture & allied sectors, Skill development etc.

10.2. Development of Integrated Check Posts (ICPs)

Border Out Posts (BOPs) are designated **entry and exit points** on the international border of the country through which cross border movement of persons, goods and traffic takes place. Inter-alia, the BOPs are meant to provide appropriate show of force to deter trans-border criminals, infiltrators and the hostile elements from indulging in the activities of intrusion / encroachment and border violations. Each BOP is provided with the **necessary infrastructure** for accommodation, logistic supports and combat functions. It also facilitates trade & commerce.

Existing infrastructure available with Customs, Immigration and other regulatory agencies at these points on our land borders needs to be upgraded. **Support facilities** like warehouses, parking lots, banks, hotels, etc. needs to be increased in numbers.

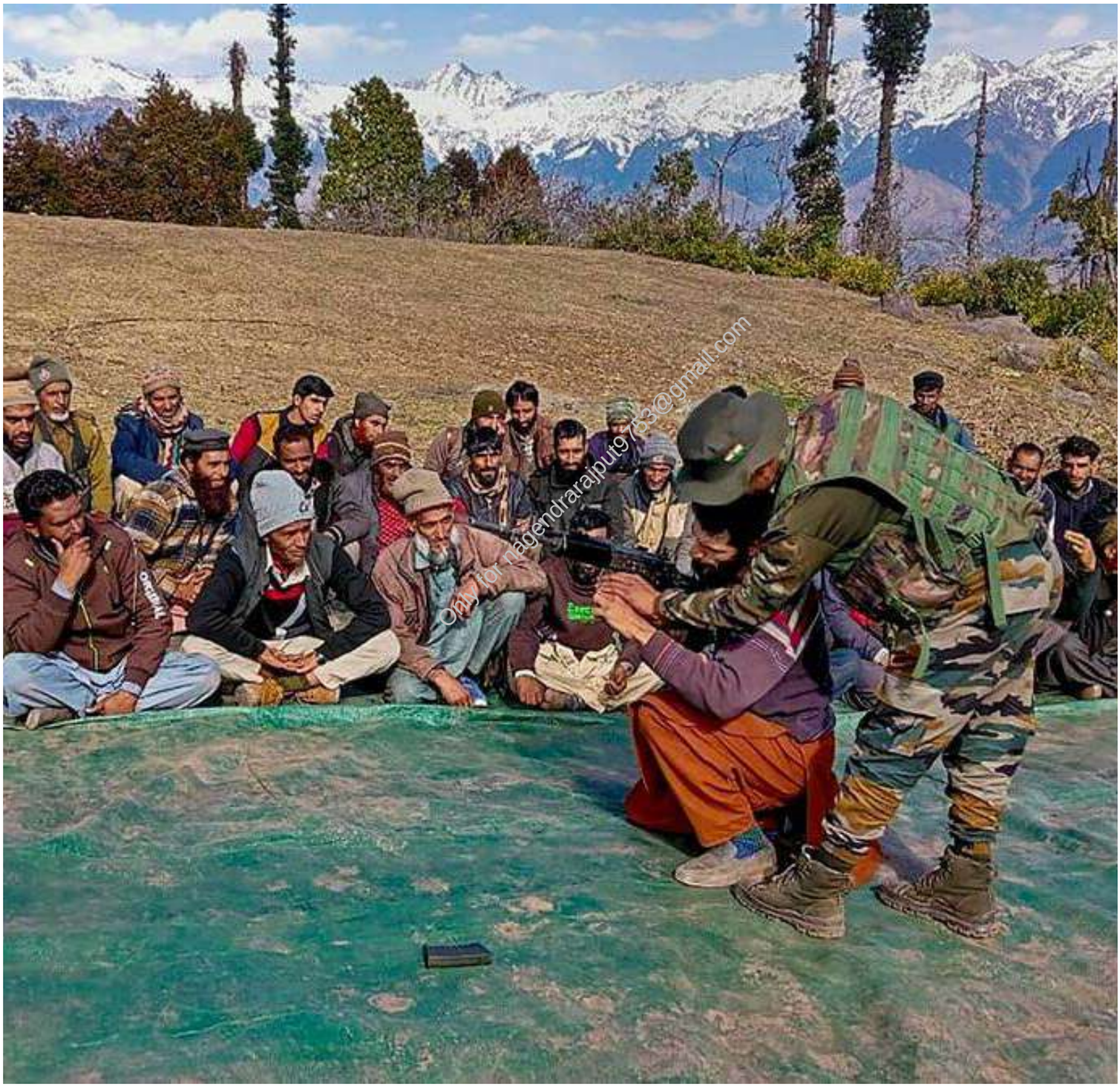
A Statutory Authority called **'Land Ports Authority of India'** (LPAI) has been set up to oversee and regulate the construction, management and maintenance of the ICPs.

The LPAI has been envisaged as a **lean, oversight body** aimed at providing better administration and cohesive management of cross-border movement of people and goods. It would be vested with powers on the lines of similar bodies like the Airports Authority of India.

10.3. Recent initiatives

- **Vibrant Villages Programme:** A Centrally Sponsored Scheme introduced in 2022 Budget, which aims to develop the essential infrastructure and creation of livelihood opportunities in certain districts and border blocks of 4 states and 1 UT namely Arunachal Pradesh, Sikkim, Uttarakhand, Himachal Pradesh and Ladakh.

- **Border Infrastructure and Management (BIM):** A **Central Sector Umbrella Scheme (2021-22 to 2025-26) which aims to provide better roads, electricity, and communication infrastructure along the border areas.**
- **Comprehensive Integrated Border Management System (CIBMS):** An integrated system that utilises high-tech surveillance devices such as sensors, detectors, cameras, radar systems to address the gaps in the present system of border security.
- **Village Defence Guards (VDG):** Earlier known as Village Defence Committees (VDC) in J&K. These function under SP/SSP with an aim to provide residents of remote hilly villages with weapons and give them arms training to defend themselves.



11. Coastal Security

India's coastline runs through **nine States** viz. Gujarat, Maharashtra, Goa, Karnataka, Kerala, Tamil Nadu, Andhra Pradesh, Odisha and West Bengal and **four** Union Territories viz. Dadra and Nagar Haveli and Daman & Diu, Lakshadweep, Puducherry and Andaman & Nicobar Islands, situated on the coast.

India's 7516 km long coast line presents a variety of security concerns that include landing of arms and explosives at isolated spots on the coast, infiltration/ex-filtration of anti-national elements, use of the sea and off shore islands for criminal activities, smuggling of consumer and intermediate goods through sea routes etc. Absence of physical barriers on the coast and presence of vital industrial and defence installations near the coast also enhance the vulnerability of the coasts to illegal cross border activities. Some instances of vulnerability of country's coasts being exploited are:

- The **smuggling of explosives** through the Raigad coast in Maharashtra and their use in the 1993 serial blasts in Mumbai, and
- The infiltration of the ten Pakistani terrorists through the sea route who carried out the multiple coordinated attacks in Mumbai on November 26,2008

Broadly, **coastal security** is understood as a **subset of maritime security** that involves securing the country's coasts by guarding its maritime approaches against any threat or challenge that originates from the sea.

11.1. Challenges

- India's coasts are characterised by a **diverse range of topography** such as creeks, small bays, back waters, rivulets, lagoons, estuaries, swamps, mudflats, as well as hills, rocky outcrops, sandbars, beaches and small islands (inhabited as well as uninhabited).
- The **physical proximity of India's coasts** to politically volatile, economically depressed and unfriendly countries such as Sri Lanka, Bangladesh, Pakistan and Gulf countries adds to its vulnerability.
- **Unsettled maritime boundaries** not only pose serious security challenges but also hinder offshore development such as India's maritime boundaries with Pakistan (Sir Creek) and Bangladesh are not delineated because of overlapping claims.

11.2. Maritime Security & Threats

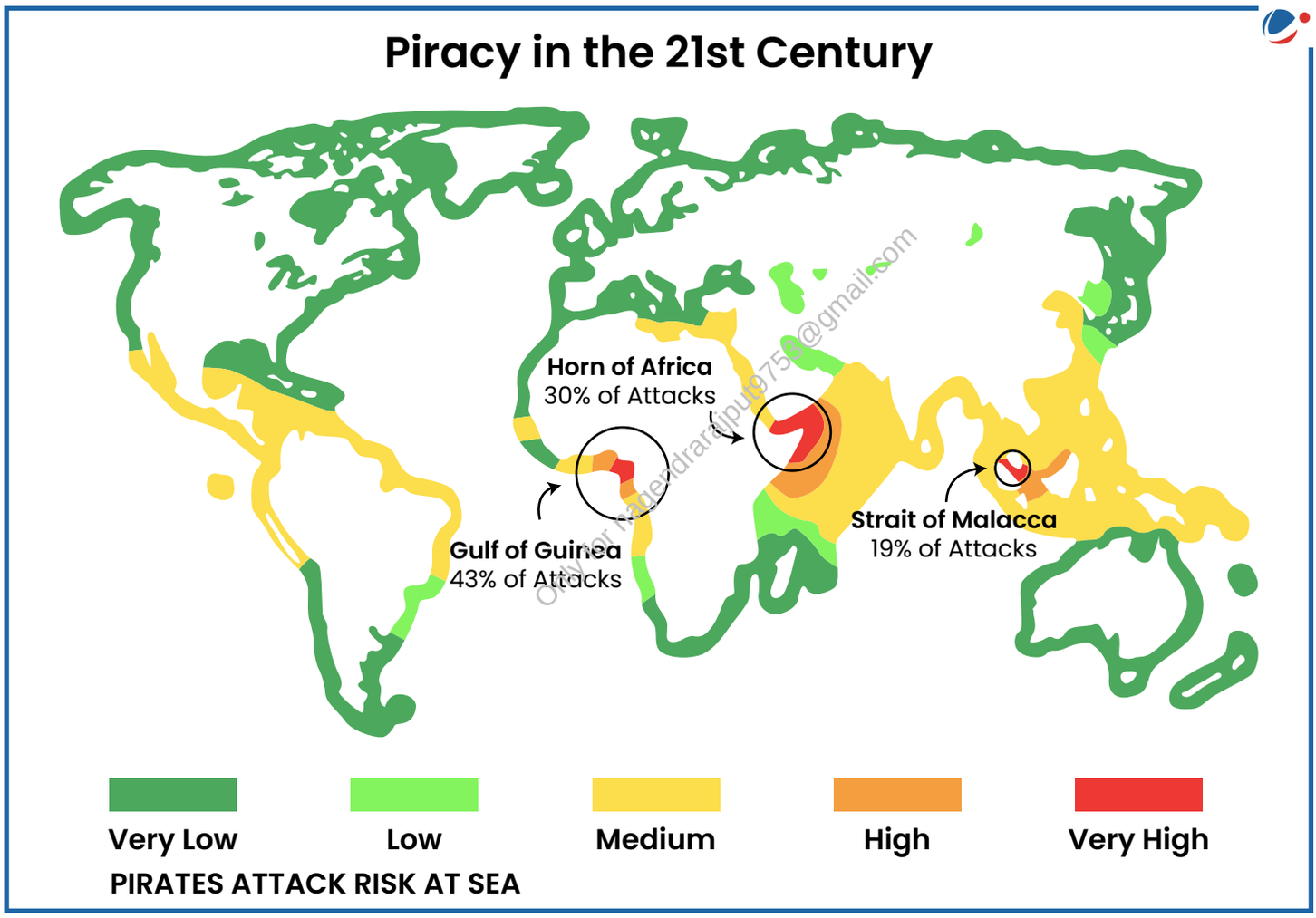
India faces a number of threats and challenges that originate from the sea and which are mainly sub-conventional in nature. These threats and challenges can be categorised under five broad categories:

1. **Maritime terrorism:** It is defined as '...the undertaking of terrorist acts and activities within the maritime environment, using or against vessels or fixed platforms at sea or in port, or against any one of their passengers or personnel, against coastal facilities or settlements, including tourist resorts, port areas and port towns or cities'.
2. **Piracy and armed robbery:** Piracy by definition takes place on the high seas and, therefore, does not fall under the ambit of coastal security. However, in the case of India, the shallow waters of the Sunderbans have been witnessing **'acts of violence and detention'** by gangs of criminals that are akin to piracy.

3. **Smuggling and trafficking:** Indian coasts have been susceptible to smuggling and trafficking. Gold, electronic goods, narcotics and arms have been smuggled through the sea for a long time. Indian coasts have been susceptible to smuggling. Gold, electronic goods, narcotics and arms have been smuggled through the sea for a long time.

4. **Infiltration, illegal migration and refugee influx:** India's land boundaries have always been porous to infiltration by terrorists/militants and large scale illegal migration. These large scale influxes over the decades have resulted in **widespread political turmoil** in the Border States. To prevent infiltration and large scale illegal migration, the Indian government implemented widespread security measures, included maintaining strict vigil along the borders, the erection offences, and the thorough checking of immigrants. The elaborate security arrangements on land forced the terrorists and illegal migrants to look towards the sea where security measures are comparatively lax, enabling them **to 'move, hide and strike'** with relative ease.

5. **The straying of fishermen beyond the maritime boundary:** The frequent straying of fishermen into neighbouring country waters has not only jeopardised the safety of the fishermen but has also raised national security concerns (as discussed in Indo-Sri Lanka).



11.3. The Coastal Security Architecture

One of the earliest challenges to coastal security that India has had to encounter was sea-borne smuggling. Alarmed by the rising graph of **sea-borne smuggling** and mindful of the inadequacies faced by the maritime law enforcement agencies, GoI created two specialized forces within a span of a few years: the Customs Marine Organisation and the Indian Coast Guard.

EVOLUTION OF COASTAL SECURITY ARCHITECTURE	
Year	Developments
1974	❯ **Customs Marine Organisation (CMO), was established** to conduct anti-smuggling operations.
1977	❯ **Indian Coast Guard (ICG), was established to prevent** smuggling activities, protecting installations, assisting fishermen and preserving marine environment.
2005	❯ **Coastal Security Scheme** with a three-layered structure to strengthen patrolling and surveillance.
Post 26/11 attack	❯ **Multilayered Surveillance System was strengthened** with ecpansion in roles and duties of Indian Navy, etc ❯ **NC31 network and IMAC** were established to strengthen maritime domain awareness ❯ **Increased cooperation with other countries** for information sharing, capacity building etc.
2017	❯ **Maritime Theatre Command is proposed** to Integrate the assets of Indian Navy Army, IAF and Coast Guard to form a Net-centric Warfare model.
2020	❯ **First national maritime security coordinator** appointed.

11.3.1. The Customs Marine Organisation (CMO)

CMO was created following the recommendations of the **Nag Chaudhari Committee.** The objective of the committee was to suggest the optimum assets required for anti-smuggling operations as well as recommend ways to curb smuggling through the sea. Once the Indian Coast Guard was formed in 1977, the CMO was merged with the newly created organisation.

11.3.2. The Indian Coast Guard (ICG)

The ICG was established on February 1, 1977 in the naval headquarters, and placed under the **Ministry of Defence (MoD).** On August 18, 1978, with the enactment of **the Coast Guard Act,** the organisation formally came into being as **the fourth armed force of India.** The Act stipulates that the ICG as an armed force would ensure the security of the maritime zones of India, and protect its maritime and national interests in such zones.

11.3.3. The Marine Police Force

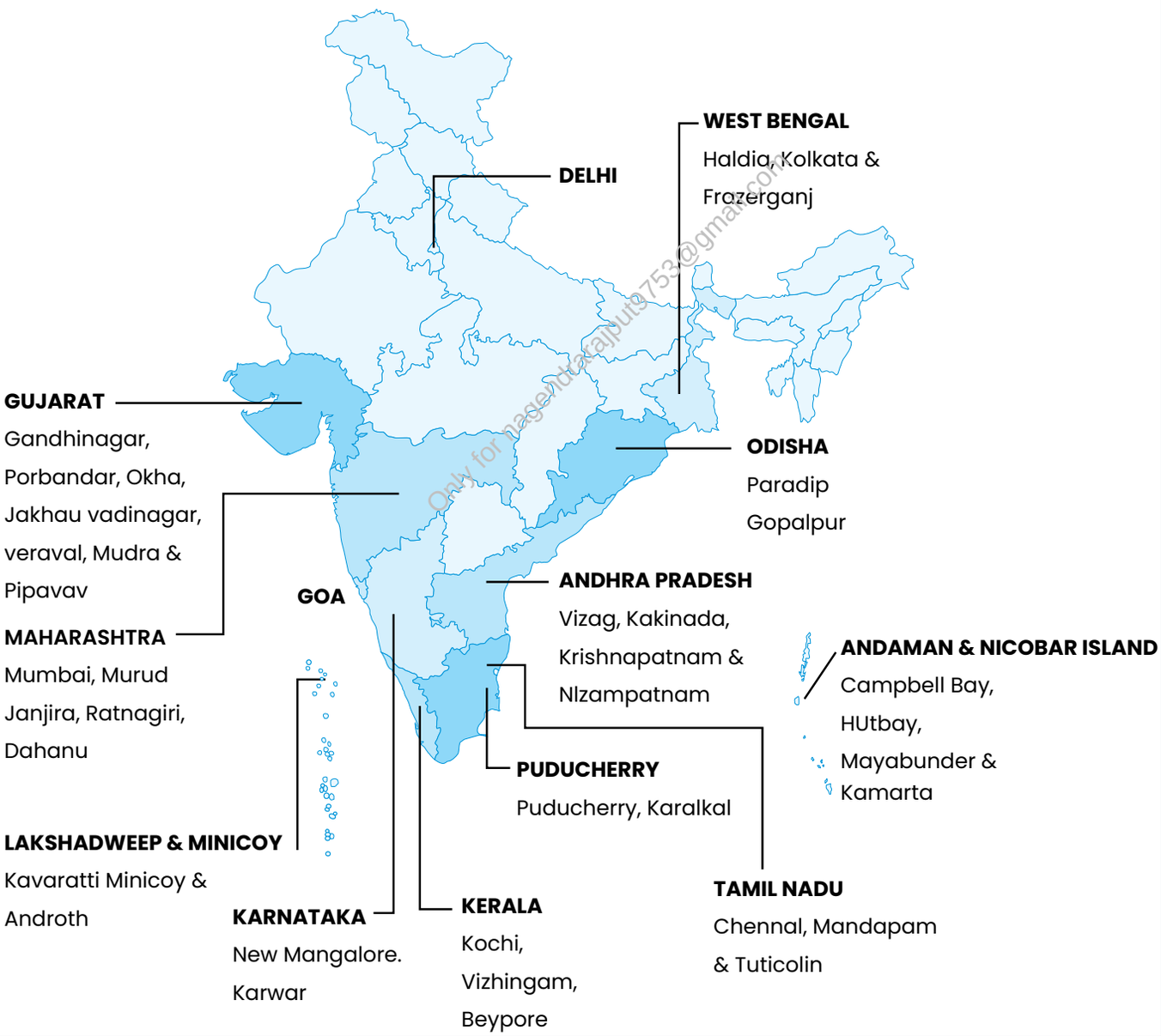
The marine police force was created under the **Coastal Security Scheme (CSS)** that was launched in 2005. The aim of the CSS was to **strengthen infrastructure for patrolling and the surveillance of the coastal areas,** particularly the shallow areas close to the coast.

The marine police force was required to work closely with the ICG under the **'hub-and-spoke' concept,** the 'hub' being the ICG station and the 'spokes' being the coastal police stations. The marine police was mandated to patrol the territorial waters (12 nautical miles into the sea) and pursue legal cases pertaining to their area of responsibility according to specified Acts.

ORGANISATIONAL COVER

Marltlme zones are divided Into 5 coast guard regions: northwest (HQ Gandhinagar), west (HQ Mumbai), east (HQ Chennal), northeast (HQ Kolkata) and Andaman & Nicobar (HQ Port Blair). Each region has 14 districts, where CG stations are housed:

COAST GUARD STATIONS



11.3.4. Present Coastal Security System

There is a multi-tier arrangement for protection and maritime security of the country involving the Indian Navy, Coast Guard and Marine Police of the coastal States and Union Territories.

- The surveillance on the **high seas** is carried out along the limits of EEZ (exclusive economic zone) by the **Navy** and the **Coast Guard.**
- In the **territorial waters**, the **Coast Guards** protect the Indian interests with vessels and through aerial surveillance.
- Close coastal patrolling is done by **State Marine Police.**

The State's jurisdiction extends **up to 12 nautical miles** in the shallow territorial waters.

11.4. Initiatives in Coastal Security Architecture

The mind-set that coastal security is not an essential component of national security eventually changed post 26/11 terrorist attacks in Mumbai on November 26, 2008.

Since 2008, coastal and maritime security has been strengthened substantially by successful implementation of technical, organisational and procedural initiatives, by all maritime security agencies. Plugging gaps, where identified, is **continuous process** that is being addressed appropriately. The Indian Navy has been the lead agency in this regard and is assisted in this task by the Indian Coast Guard, Marine Police and other Central and state agencies. Steps taken are:

- **Indian Maritime Security Strategy (IMSS) 2015 of Indian Navy:** It envisages greater coordination between different maritime agencies; securing Indian Ocean sea lines of communication (SLOCs); Maritime Security Operations for contemporary assessments of maritime terrorism, piracy etc.; multilateral maritime engagement, local capacity building, technical cooperation etc.
- **Coastal Security Scheme (CSS)** is being implemented to strengthen security infrastructure of Marine Police Force in coastal states/UTs. It aims to strengthen **Surveillance through Automatic Identification System (AIS) receivers** and a chain of overlapping coastal radars, for gapless cover along the entire coast.
- **Coordination-** At the apex level the **National Committee for Strengthening Maritime and Coastal Security (NCSMCS),** headed by the Cabinet Secretary, coordinates all matters related to Maritime and Coastal Security. Inter–agency coordination, between nearly 15 national and state agencies has improved dramatically, only due to regular "exercises" conducted by the Navy in all the coastal states.
- **Joint Operations Centres (JOCs)-** are set up by the Navy as command and control hubs for coastal security at Mumbai, Visakhapatnam, Kochi and Port Blair are fully operational. These JOCs are manned 24×7 jointly by the Indian Navy, Indian Coast Guard and Marine Police.
- **Coastal Surveillance Network,** comprising of static sensors along coasts, automatic identification systems (AIS), long range tracking, day-night cameras and communication devices has been put in place. **Vessel Traffic Management System (VTMS) radars** are installed on all major & minor ports to facilitate surveillance.
- **Enhance Maritime Domain Awareness:** through National Command Control Communication and Intelligence Network (NC3I), an over-arching coastal security network which collates and disseminates data about all ships, dhows, fishing boats and all other vessels operating near our coast.

- **Activities in maritime zones are now more regulated:** (i) Multi-purpose ID issued to all fishermen, sea ferrying services and coastal villages (ii) Uniform licensing of fishing boats (iii) GPS and transponders for tracking.
- **Operation Sagar Kavach** was put in operation post 26/11 to improve coordination between security agencies including Indian Navy, Coast Guard and the local police.
- **Indian Ocean Naval Symposium** (IONS; 25 Members & 09 Observers) was conceived by Indian Navy in 2008. It is a voluntary initiative that seeks to increase maritime co-operation among navies of the littoral states of the Indian Ocean Region.
- The Indian navy also raised a specialised force called the **Sagar Prahari Bal** in 2009 for protecting its bases and adjacent vulnerable areas and vulnerable points.
- **Information Fusion Centre – Indian Ocean Region (IFC-IOR)**
  - It is a regional maritime security centre hosted by the Indian Navy, established in 2018 in Gurugram.
  - Objective: To enhance maritime domain awareness and share information on vessels of interest.
  - Region covered: Indian Ocean Region and adjoining Seas.
  - Significance: Enhancing global efforts to combat maritime security threats including Piracy & Armed Robbery, Contraband (illegal goods) Smuggling, IUU (Illegal Unregulated and Unreported) Fishing, etc.

  - Currently, the IFC-IOR has International Liaison Officers (ILO) from 12 partner nations.
    - » Australia, France, Italy, Japan, Mauritius, Myanmar, Seychelles, Singapore, Sri Lanka, United Kingdom, United States.
- **Training –** The Navy and Coast Guard have also provided periodic maritime training to marine police in all coastal states. In order to have a permanent police training facility, Marine Police training institutes in Tamil Nadu and Gujarat have been approved by the Government.
- Involving fishermen in surveillance & intelligence gathering: **Fishermen groups,** referred to as the 'ears and eyes' of coastal security, are created comprising of trained volunteers who monitor the seas and coastal waters.
- **Electronic Surveillance** to provide near gapless surveillance of the entire coastline as well as prevent the intrusion of undetected vessels under the **coastal surveillance network project.** The network comprises the Coastal Radar Chain, the Automatic Identification System (AIS), and VTMS.
- **Harbour Defense And Surveillance System –** Indian Navy has installed Integrated Underwater Harbour Defense and Surveillance (IUHDSS) at Mumbai and Vishakhapatnam naval harbour. Designed by Israeli Aerospace Industry called ELTA, it comprises of Coastal Surveillance Radars, High Power Underwater Sensors and Diver Detection Sonars.
  - It is capable of **detecting, identifying, tracking and generating warnings** for all types of surface and subsurface Threats to harbor security. This integrated system (already installed at Kochi and Visakhapatnam) will enhance the security of naval dockyard of Mumbai by providing the comprehensive real-time images for monitoring and analysis.

Anti-Maritime Piracy Act, 2022

- The Act defines piracy as "any illegal act of violence or detention or any act of depredation committed for private ends by any person or by the crew or any passenger of a private ship and directed on the high seas against another ship or any person or property on board such ship".
- The Act will apply to high seas which includes EEZ and all waters beyond the jurisdiction of any other state
- The accused can be transferred to any country for prosecution with which India has signed an extradition treaty.
- Central Government, in consultation with the Chief Justice of the concerned High Court, will specify certain courts as Designated Courts for speedy trial of offences of piracy.
- Only authorized personnel are allowed to carry out arrest and seizure of the Pirate ships.
- Ship or property seized will be disposed of only by a Court order.

Significance of Anti-Piracy Act

- India being a signatory to the United Nations Convention on Laws of Seas (UNCLOS), is expected to cooperate in controlling the menace of Piracy all around the world.
- Growing menace of Piracy along the Gulf of Aden, which is the major gateway connecting Asia, Europe and East coast of Africa.
- India does not have a specific law or legal provision in Indian Penal Code or Criminal Procedure Code for piracy.
- Need to provide maritime security as more than 90 percent of India's trade is through sea routes and more than 80% of our hydrocarbon requirement is ferried through sea route.

11.5. Way forward

Being a coastal nation, India has been witnessing a range of maritime activities taking place along its coasts and adjacent waters over the ages. However, activities such as the smuggling of precious metals and items, trafficking of arms and drugs and the infiltration of terrorists have adversely impacted the country's economy as well as its security.

- The Coast Guard should be designated as the single authority responsible for coastal security.
- Strengthening of the Coast Guard (CG): 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.
- Stronger involvement of coastal police: State police agencies may be integrated in the detection and capture of criminals at sea leveraging their unique access to fishermen and local communities, facilitating the flow of vital human intelligence.
- The MHA should concentrate on the issue of training the marine police (developed under the coastal security scheme (CSS) in 2005-06) as its next step. It should set up specialised marine training institutes in the country, which will provide a comprehensive and uniform course in sea-faring, sea-policing, sea-navigation as well as laws and regulations pertaining to crimes at sea.
- The Indian navy should be eased out from coastal security responsibilities and allowed to concentrate on developing its blue water capabilities and defending the country during times of war.

12. Conclusion

The proper management of borders, which is vitally important for national security, presents many challenges and includes coordination and concerted action by administrative, diplomatic, security, intelligence, legal, regulatory and economic agencies of the country to secure the frontiers and sub serve its best interests.

On the lines of many developed countries, there is a need to adopt a **participative and multi-national integrated border management system** in India. People oriented measures (Involvement of Stakeholders) should be taken such as :

- **Community Participative Border Management, sensitive to the varied cultures.** This would require preventing alienation of border population. **Community policing and Village defence and development committees** would also go a long way in achieving secure borders.
- **Community development by Border Guarding Forces (BGF).** This would help earn the goodwill of people. For example, In 2004, as part of **Operation Sadbhavana**, projects were undertaken to electrify remote rural villages and hamlets with solar panels and windmills and provide job opportunities to the poor people of backward areas of Jammu and Kashmir.
- **Enhancement of border trade** with neighbouring countries for the benefit of the people. Flourishing border trade will promote peaceful borders in the long run.
- **Employment opportunities locally:** It will prevent the pull towards illegal activities like drug or arms trafficking.

The **Madhukar Gupta Committee** recommendations to strengthen border protection along Indo-Pakistan Border also need to be considered. It suggests measures such as replacing "linear security" by **"grid border protection";** better coordination by BGF with local police and Intelligence generation.

The concept of **Village Volunteer Forces (VVFs)** helping in border management has a great deal to commend itself and has worked with a good degree of success in areas where it has been tried so far. India should promote it further.

13. UPSC Mains Previous Years Questions

1. What are the maritime security challenges in India? Discuss the organisational, technical and procedural initiatives taken to improve the maritime security. (2022)
2. 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. (2020)
3. Cross-border movement of insurgents is only one of the several security challenges facing the policing of the border in North-East India. Examine the various challenges currently emanating across the India-Myanmar border. Also discuss the steps to counter the challenges. (2019).
4. Border management is a complex task due to difficult terrain and hostile relations with some countries. Elucidate the challenges and strategies for effective border management. (2016)
5. How does illegal transborder migration pose a threat to India's security? Discuss the strategies to curb this, bring out the factors which give impetus to such migration. (2014)
6. How far are India's internal security challenges linked with border management, particularly in view of the long porous borders with most countries of South Asia and Myanmar? (2013)

14. Vision IAS Mains Previous Years' Questions

1. Examine the implications of illegal migration on India's internal security. Discuss the measures currently in place to mitigate the associated security challenges.

Approach:

- Define illegal migrants and highlight the increasing trend of illegal migration in the recent years.
- Examine the implications of illegal migration on India's internal security.
- Discuss the legal measures in force to tackle this issue.
- Conclude accordingly.

Answer:

As per the Citizenship Act, 1955, an **illegal migrant** is a **foreigner who enters the country without valid travel documents,** or who enters with valid documents but **overstays the permitted time period.**

In the recent years, ethnic violence against Rohingyas in Myanmar, religious persecution of minorities in Pakistan and Afghanistan, and a porous border with Bangladesh have led to increasing concerns about the influx of illegal migration into India.

The entry of illegal migrants into India poses the following security threats:

- **Changing demographics:** Large-scale illegal migration risks altering the demographic balance, potentially leading to the **destabilization of a region.**
  - *For example, the communal violence in Bodo areas of Assam and demand for Bodoland highlight the issue of changing demographics of the region due to illegal migrant influx.*
- **Risk of radicalization and terrorism:** Social and economic marginalization of migrant communities can create a fertile ground for extremist ideologies to take root and be used for terrorist activities.
  - *For example, suspected linkages of Rohingya migrants with Pakistan-based terror organisations such as Lashkar-e-Taiba and Jaish-e-Mohammed.*
- **Smuggling and human trafficking:** Illegal migration has created hotspots in areas bordering Myanmar, Pakistan, and Bangladesh, leading to an increase in smuggling of arms and drugs, as well as increase in human trafficking.
  - *For example, arms smuggling via Myanmar and Pakistan borders and trafficking of women from Nepal into India.*
- **Proxy for external actors:** Illegal migrants can serve as conduits for information and support to hostile external groups.
  - *For example, ISI's alleged use of illegal migrants in the Indian territory for operations in India.*

Existing measures to tackle illegal migration are:

- **Border management and fencing:**
  - The government has launched the **Comprehensive Integrated Border Management System** to control cross border crimes like illegal infiltration, cross border terrorism, etc. Moreover, border fencing has been erected on the Indo-Pakistan border and Indo-Bangladesh border.
  - **Integrated check posts** have been constructed on India-Bangladesh, India-Nepal borders, etc. to check the influx of illegal migration and prevent human trafficking.

- **Legal framework:** The government has taken various legal measures to address the issue of illegal migrants. For example:
  - **The National Register of Citizens (NRC)** process initiated in Assam aims to identify and exclude illegal immigrants. It was updated in 2019 to identify illegal migrants.
  - **The Foreigners Act, 1946** enables the government to form tribunals with the authority to decide whether a person is a foreigner or not.
- **Intelligence sharing:** India collaborates with intelligence agencies from neighbouring countries to track and apprehend illegal migrants.
  - For example, **regular exchange of information between India's and Bangladesh's security agencies to track activities of extremist groups.**

Illegal migration significantly impacts India's internal security by posing threats to national security, law and order, and social stability. Addressing this issue requires a comprehensive approach that includes **strengthening border controls, enhancing surveillance, and implementing effective measures to regulate migration.**

2. What is the role played by the Indian Coast Guard (ICG) in safeguarding the maritime security of India?

Approach:

- Introduce by providing a brief account of the Indian Coast Guard (ICG).
- Highlight the role of ICG in safeguarding India's maritime security.
- Conclude appropriately.

Answer:

India is primarily a maritime nation with a long coastal boundary of 7516 km. Owing to its strategic location in the Indian Ocean Region (IOR), the Indian Coast Guard (ICG) was formally established under the **Coast Guard Act, 1978** with a mission of protecting offshore resources, assisting mariners in distress, enforcing maritime laws against poaching, smuggling, and narcotics, etc.

Role of ICG in safeguarding the maritime security of India

- **Maritime patrol and surveillance:** The ICG utilizes its extensive surveillance capabilities to monitor India's maritime borders. It employs advanced technologies like the **Coastal Surveillance Network** (CSN) and **Automatic Identification System** to detect and deter potential threats effectively.
  - *For example, ICG was designated for **coastal security post-Mumbai attacks in 2008,** including the task of coordinating between central and state agencies. It implements CSN for effective surveillance and response.*
- **Maritime law enforcement:** As a maritime law enforcement agency, the ICG actively combats criminal activities through interception and apprehension of offenders.
  - *For example, ICG, in carrying out anti-smuggling and Narcotics control at sea, has **seized contraband worth Rs. 15343 crores** (including Rs 478 crores in 2023).*
- Cooperation with regional partners: The ICG collaborates closely with regional Coast Guard agencies through joint exercises, patrols, and information-sharing mechanisms.
  - *For example, India regularly conducts joint exercises with its neighbours to strengthen the **"SAGAR" and "Neighbourhood First" policies** of the Indian Government.*
- **Enhance maritime domain awareness:** By closely monitoring vessel movements, the ICG enhances maritime domain awareness, enabling timely detection and deterrence of potential non-traditional security threats such as illegal fishing, piracy, and illicit trafficking.

- *For example, the ICG **prevents illegal fishing** by foreign vessels within **India's Exclusive Economic Zone (EEZ).***

- **Ensures comprehensive security matrix:** The security matrix of ICG enables it to address coastal security, offshore security, anti-terrorism, anti-piracy and port security. The ICG also provides support to the Indian Navy to ensure the maritime security of the country.

Given the increasing significance of IOR and the need for a greater presence of India in this region, the importance of ICG has seen further enhancement. The government of India in this regard is making efforts to strengthen its capability and reach to make it a critical pillar of India's maritime security and economic development.

3. An unmanaged border accentuates threats from unconventional sources by providing easy points of ingress and egress. Discuss in the context of India's international border along the north eastern states.

Approach:

- Give a very brief account of vulnerability to North Eastern Region to unconventional threats.
- Second part should discuss in detail the border management in the NE region.

Answer:

The NE Region of India is vulnerable due to its

- peculiar geo-strategic location,
- hostile elements inhabiting the region, and
- porous borders with neighboring countries.

The porous nature of these borders, which pass through difficult terrain of forest, rivers and mountains, make the task of guarding all the more challenging.

The NE borders with our neighbors poses different challenge owing to varying nature of our relations. In an increasingly interconnected world it is the unconventional sources that present a greater threat. These threats are:

- **Militancy:** The presence of militant outfits in most of the North Eastern States and their ability to indulge in hit and run operations across borders is detrimental to both inter-state and intra-state relations.
- **Drug Trafficking:** Due to their proximity to the "Golden Triangle" (Drug haven in Southeast Asia) has led to growing incidence of substance abuse and drug trafficking in the NE states.
- **Smuggling:** While the issue of human, cattle smuggling and counterfeit currency in Indo-Bangladesh border is the main threat, it is illegal arms and narcotics that passes through porous Indo- Myanmar border and destabilize the whole region.
- **Illegal Migration and human trafficking:** Improperly managed borders have led to unhindered migration from neighboring countries, severely impacting the demography of the region. Further, there have been cases of human trafficking from across the border.

The Indian government started fencing of Bangladesh border from 1985 onwards to curb illegal migration. Simultaneously, efforts have been done in collaboration with the Myanmar government to conduct joint operation for destroying safe havens and militant training camps.

The Government has taken the following measures:

- **Increased cooperation with some neighbouring countries:** For example, "Operation All Clear" of 2003 by the Bhutanese Army flushed ULFA's cadres out and India's borders with Bhutan are more or less secure today. The Land Boundary Agreement with Bangladesh is another example.
- **Strengthening of the Department of Border Management:** The department has been entrusted with the task of fencing of the borders in NE region on priority. The Border Area Development Programme has been expanded to cover the border blocks of the 8 North Eastern states as well.
- **Setting up of Integrated Border Check Posts:** India and Bangladesh are in the process of setting up integrated check posts, along with the development of the regional economy. This is expected to reduce anti-India activities.

Challenges to effective border management

- Geographical reason – Difficult terrain, marshes, rivers, etc.
- Infrastructural gap in the eastern region
- Stability of relation with neighbors is affected by the change of regimes and/or stability with the adjoining states. For example: Bangladesh government changes, Junta rule in Myanmar have a prominent effect on our relationship and consequently effects border management also.
- Manpower and Funding.
- Land acquisition (in Meghalaya and Tripura) and environmental clearance (Mizoram) delays
- Lack of economically integrated with the rest of country.
- Border demarcation especially along China border.

Suggestions

- Flood light system along the fence. Floating fences across river streams.
- There is a need to settle friendly population along the fencing as a second line of defence.
- Friendly relations with neighboring countries, as far as sound border management is concerned, have to be vigorously pursued.

Since India's international borders in the North East present an interesting mix of both friendly and unfriendly neighbours, a far greater effort needs to be put into the entire strategy of border management. While India's North East stands to gain from a cooperative framework in the region, important issues of security and development can only be addressed through effective border management.

4. Discuss the security threats present in the Indian Ocean Region (IOR), which have a direct bearing on India's maritime border interests. Suggest a robust strategy to deal with these threats.

Approach:

- Write about the Indian Ocean Region (IOR) in introduction.
- Discuss the maritime security concerns that India faces in the IOR.
- Write about persistent efforts and a robust strategy needed to address the concerns.
- Conclude accordingly.

Answer:

The Indian Ocean Region (IOR) extends from the eastern coast of Africa to the western coast of Australia, and accounts for one-fifth of the water on Earth's surface. India has a long coastline of more than 7500

km in the Bay of Bengal and the Arabian Sea and sits at the head of the Indian Ocean. Indian Ocean Region is of prime importance for India but it is replete with security concerns as given below:

- **Choke Points:** Transit routes in the region are connected through important choke points, such as the Straits of Malacca, Straits of Hormuz, Bab el Mandeb, etc. and they raise concern as they increase the vulnerability of supply chain disruption.
- **Maritime Piracy:** The concentration of piracy activity around major maritime passages such as the Straits of Hormuz and the Gulf of Aden illustrates the risks associated with geographically constrained transit points in terms of blockades and hijacking of ships, thus posing security threats to international trade.
- **Drug Trafficking:** The Indian Ocean Region is in near proximity to areas of drug production, the Golden Crescent and the Golden Triangle, which makes it susceptible to illicit activities like drug trafficking.
- **Illegal criminal activities:** Criminal activity, such as illegal, unreported and unregulated fishing (IUUF), trafficking in persons, smuggling of migrants etc. often takes place in the Indian Ocean Region, thus raising security concerns for India.
- **Growing Chinese Presence:** The expanding Chinese Navy through its Maritime Silk Road has acquired many ports, naval bases such as Djibouti; Gwadar etc. which reflects the growing military ambitions of China in the otherwise peaceful Indian Ocean region.

In order to address these security concerns, which have direct bearing on India's maritime border interests, persistent efforts and a robust strategy is required as given below:

- **Bolster regional maritime security framework:** India can work towards strengthening the Indian Ocean Rim Association (IORA), and creating inherent linkages with Indian Ocean Naval Symposium (IONS) to ensure effective implementation of actions for strengthening maritime security.
- **Foster strategic relations at choke points:** It is important to build strategic relationships with littoral nations in such regions to address India's Maritime Security concerns and ensure unhindered and unimpeded flow of Indian trade and shipping for continued economic progress.
- **Intelligence Sharing:** Mechanisms and protocols for exchange of tactically important information and intelligence need to be put in place for interdiction and prosecution of vessels and persons engaged in illegal activities.
- **Coordinated Patrols and maritime exchanges:** In the absence of regional or sub-regional security architecture, bilateral and multilateral exchanges like the MILAN series of exercises, in all spheres of the maritime security domain between concerned agencies of various littoral nations of IOR can be promoted.
- **Anti-Piracy efforts:** India needs to take the lead in establishing a sub-regional mechanism for the North-Eastern IOR with the participation of Bangladesh and Myanmar to curb piracy.

India being the largest nation in the IOR has the responsibility to drive the security apparatus in the region tempered with the current geopolitical realities and the aspirations of the other states. In this regard, India has taken key steps such as **Security and Growth for all in the Region (SAGAR), Information Fusion Centre for Indian Ocean Region (IFC-IOR)** etc. which plays a vital role in enhancing regional collaboration for addressing the maritime security challenges.

5. Why is ensuring maritime security considered the key to safeguarding India's strategic and economic well-being? What is the significance of the Maritime Anti-Piracy Act in this regard?

Approach:

- Discuss the importance of maritime security for India.

- Highlight the significance of the Maritime Anti-Piracy Act in this context.
- Conclude accordingly.

Answer:

India has a coastline of over 7500 km, which makes maritime security an important aspect of national security. **Ensuring maritime security is the key to safeguarding India's strategic and economic well-being due to the following reasons:**

- **Maintaining balance of power:** The unchallenged rise of authoritarian China casts a serious shadow on security dynamics of India and in this context, maritime power plays a vital role in ensuring geo-political stability and progression of geo-economics.
- **Safeguarding strategic choke points:** Ensuring maritime security is necessary to secure sea lines of communications, to secure choke points, thus leading to freedom of navigation and resolving conflicts peacefully.
- **Trade and energy security:** Ensuring maritime security is necessary, as more than 90 percent of India's trade and more than 80 percent of hydrocarbon requirement is ferried through sea routes.
- **Ensuring zone of peace:** India's vast coastline presents numerous security challenges like piracy, illegal landing of arms and explosives, infiltration, drug and human trafficking and smuggling. Ensuring maritime security is vital to address these challenges and ensure peace in the region.
- **Ensuring sustainable use of resources:** Maritime security is necessary to protect the resource wealth of the ocean and ensure its use in a sustainable manner.

In this context, The **Maritime Anti-Piracy Act, 2022, which received the President's assent in 2023** is a key step and has the following **significance:**

- **Maritime security:** The Act seeks to enhance the existing maritime security operations in the Indian Ocean region. It will help tackle the growing menace of piracy along the Gulf of Aden, which is the major gateway connecting Asia, Europe and East coast of Africa.
- **Compliance with UNCLOS:** It is believed that the Act will strengthen international cooperation and regional partnerships to combat piracy in the region, ensuring proper compliance with the United Nations Convention on the Law of the Sea (UNCLOS).
- **Specific law:** This Act represents India's first piece of domestic legislation specifically written to criminalise maritime piracy on the high seas and allows Indian authorities to respond.
- **Wide coverage:** It applies to the high seas, which under the Act includes the Exclusive Economic Zone and all waters beyond the jurisdiction of any other State.
- **Provision of punishment:** Committing an act of piracy is punishable with life imprisonment; or death, if the act of piracy causes or seeks to cause death, thus providing provision of stringent punishment under the law.

Ensuring maritime security is a key to safeguard India's overall security, as having a piracy-free Indian Ocean region is essential for the growth of maritime trade in the region and this will help India establish its regional supremacy.

6. India needs a smart border management system to balance legitimate cross border flows with national security interests. Discuss. Also, highlight the initiatives taken by the government in this regard.

Approach:

- Briefly define smart border management for India.

- Mention the need for a robust smart border management system.
- Highlight the steps taken by the government in this regard.
- Conclude with a way forward.

Answer:

Smart border management calls for a **balanced use of humans and technology** to **facilitate the movement of people and goods across borders, while controlling and preventing malicious acts such as infiltration, cross-border terrorism, illegal immigration and smuggling.** It entails a **coordinated and focused approach** by the country's leadership, bureaucracy, security forces and economic agencies of the nation.

Need for a smart border management system in India:

- **Long borders:** India has a long land and coastal borders of approximately 15000 Km and 7500 km respectively. Thus, managing the border in itself is a very complex task.
- **Unsettled boundaries:** The conflicts with China (Aksai Chin); Nepal (Kalapani dispute), etc. indicate the need for a robust and smart border management.
- **Difficult and diverse terrain:** Indian borders run through plains, hills and mountains, deserts, riverine territories and marshes, which make manual supervision and surveillance a tedious task.
- **Poor connectivity to hinterland:** This creates a major challenge, especially in case of standoff as seen in the recent past. It becomes very difficult to ensure the supply of important articles to remote border areas due to absence of infrastructure.
- **Illegal migration:** Several of India's neighbours are undergoing political and economic instability, which has increased the inflow of migrants. This leads to an altered demographic ratio and communal tensions within the society.
- **Crimes and syndicates:** There is rampant smuggling of contrabands, arms and ammunition drugs etc. in the border areas.

Countries in India's neighbourhood share a common history with it. There is a socio-cultural connection between the people of India and many of these countries. Thus, smart border management will ensure proper security while enhancing the cross-border movement of not only people but also of goods and services. In this regard, the government has undertaken following initiatives:

- **Comprehensive Integrated Border Management system (CIBMS)** has been employed.
  - It is a five-layer security system with the objective of implementing the **D4R2 (deter, detect, discriminate, delay, response, recover)** principle on the border.
  - The CIBMS uses low-light CCTV cameras, thermal imaging, night-vision devices (NVDs), surveillance radars, laser beams and underground monitoring sensors to detect infiltration via land, underwater, air and tunnels.
  - It includes the **integration of manpower, sensors, networks, intelligence** and command & control solutions to improve situational awareness at different levels of the hierarchy in the border guarding forces to facilitate prompt and informed decision making and quick response to emerging situations.
- **Perimeter Intrusion Detection System (PIDS)** comprising multiple types of sensors and/or Long-Range Reconnaissance and Observation Systems (LORROSs) have been installed or are in the process of deployment in strategically crucial regions. These have proven to be effective in the detection, identification, classification and recognition of intruders or other threats.

- The Department of Border Management (DoBM) is implementing the **Coastal Security Scheme (CSS)** in phases with the objective of strengthening the infrastructure and capabilities of Coastal Police for the patrol and surveillance of coastal areas, particularly shallow areas close to the coast.
- To address the issue of poor connectivity of the border areas, the government has undertaken **phase-wise construction of road links** along the border with the involvement of BRO, CPWD, PWD, etc.

The Government has taken necessary steps in this direction, yet there is a need to ensure that all the stakeholders work in close coordination with each other. Any lapse in border management can lead to major security issues as found out during the Mumbai attacks of 2008.

7. India's border with Bangladesh is particularly notorious for its porosity which has led to illegal migration. Comment. Also discuss the challenges in identifying illegal immigrants in the region and deporting them. Critically analyse the feasibility of sealing the border with Bangladesh to solve this problem.

Approach:

- Introduce with illegal migration from Bangladesh and consequently emerging problems.
- Discuss the challenges in identifying illegal immigrants in the region and deporting them.
- Critically analyse feasibility of sealing the border with Bangladesh to solve this problem.
- Conclude suitably.

Answer:

Migration from Bangladesh to bordering Indian states is not a new problem and is in continuation since independence. This issue had been raise by these state governments but nothing much could be done to solve the accompanying problems which surfaced up with time which are:

- Changing demography of the region.
- Burden on scarce resource present in the region.
- Illegal trade which is being carried out by these migrants.
- Social problems arising due to different ethnicity, religions etc.of the migrants.

This issue is not heading towards an end because of following problems in identification of these migrants such as:

- These migrants speak the same language and share same ethnicity which makes it hard to identify them.
- They have acquired documents like Ration Card and have become regular beneficiary of these services which is another problem.
- These migrants do not live in the same area for longer ad keep on roaming and today they are present from Kashmir to Kanyakumari.
- Political sensitivity of the matter does not allow the government to take tough steps and they are seen as vote bank.

According to the Assam Accord of 1985, illegal migrants who had entered Assam from Bangladesh after March 25, 1971, were to be detected and deported. The issues w.r.t. deportation are:

- Bangladesh may not accept illegal migrants as its citizen.
- Even if they are deported, porous border allows them to re-enter India again.

- Some of the states see them as their vote bank and are not ready to deport them at all.
- Lack of any mutual agreement between governments and lack in India's persuasive power is another reason.
- People have families living on both sides of the border and they visit BORDER HAATs hence deporting them is a challenge.

Since it is known attempts after attempts to solve this issue are ending up in failure , sealing the border and maintaining strict vigil along the border may offer a feasible solution.

However, at places, India has a riverine border with Bangladesh with the river Brahmaputra shifting its course very often. This makes border fencing a challenge. Secondly the area is densely populated and people on both sides live in close proximity to the border. Thus physical barrier may be easily destroyed by humans or due to riverine action.. Digital fencing through laser beams, Night vision cameras etc. offer an alternative. At the same time it is important that talks must go on from both sides to solve the issue in the long run. Efficient verification mechanism within a proper legal framework is also required, not only to stop illegal immigration, but also to promote greater regional integration.

However, fencing should be seen as a short term measure and should pave way for greater connectivity and development of collaborative infrastructure like border roads and Haats along the border areas. This will not only improve ties with Bangladesh, but will offer greater trade and employment opportunities for N-E and Bangladeshi population.

8. Enumerate the problems faced by the Indian security forces in securing our border with Pakistan. Is complete sealing of the India-Pakistan border the solution to these problems? Comment in light of the recommendations of the Madhukar Gupta Committee.

Approach:

- Describe the challenges that India has faced on its western frontier.
- Go into the merits and demerits of the idea of sealing borders with walls or fences. One may take examples of borders of other countries.
- Bolster your argument with the recommendation of the committee.

Answer:

India's border with Pakistan is nearly 3323 km long from Gujarat to Jammu & Kashmir, the characteristics of which create the following challenges in border management:

- **Challenges from across the border:**
  - Recurrent ceasefire violations by the Pakistani forces.
  - Numerous infiltration attempts by terrorists from across the border.
  - Illegal activities such as drug trade and smuggling.
- **Physical challenges:**
  - Gaps in existing fence caused by snowfall, torrential rains and overflowing rivers and shifting sand dunes.
  - Varying geography of the border from high snowy mountains of Himalayas to scorching desert of Thar.
- **Challenges of legal basis of border management:**
  - The **India Pakistan Ground Rules,** 1960-61 for the management of the International Border remains unsigned by the two sides.

- The **Ceasefire Agreement** of 2003 remains unwritten and informal.
- Adding to the wow of multiplicity of agreements is the **Karachi Agreement** over which the two governments continue to have differences.

Challenges of the Border Guarding Forces:

- The personnel are inadequate in numbers, which leads to hardships and low morale consequently.

After the report submitted by Committee on Security and Border Protection (Madhukar Gupta Committee), the Union Minister of Home Affairs announced the complete fencing of the Indo-Pak border by 2018. This will include a border security grid with a provision for real-time monitoring of the entire length of the border and capability for intervention.

While the step will help tackle many of the challenges mentioned above, there are other issues which cannot be addressed in this manner, such as

- The legal basis of border management and issues within the Border Guarding Forces remains to be addressed.
- Given the length of the border, the terrain conditions and socio-economic milieu in the border regions as well as the engineering efforts involved would make the border sealing exercise a stupendous task.
- In particular areas, such as the marshes of the Rann of Kutchh, fencing will not be possible.
- The sealing of the border will impact of trade and intercourse in the border areas.
- Heavy snows especially in north Kashmir destroy fences annually because of avalanches.
- Pakistan employs heavy cross-border firing to assist the infiltration and terrorists uses explosives to make gaps in the fencing or dig holes under the fence.
- Use of radars, as done along US – Mexico border to detect smugglers, has the danger of giving away the electronic signatures of the equipment to enemy.

Certainly, sealing of the border with fences is not the complete solution; it needs to be augmented with various technologies such as CCTV cameras, thermal image and night-vision devices, battlefield surveillance radar, UAVs, underground monitoring sensors and laser barriers. In this context, the Comprehensive Integrated Border Management System (CIBMS), as 5 layered surveillance system, must be expedited throughout the border length.

We need smart border management where vulnerabilities are tackled in a comprehensive manner by resolving all legal challenges, utilising state-of-art technologies, and deploying adequately trained man power with high morale.

9. Although open borders facilitate cultural continuity and greater interaction, their security implications cannot be undermined. Discuss the statement in context of India's open border policy with Nepal and Bhutan.

Approach:

- Give a brief overview of India's open border policies with Bhutan and Nepal
- Briefly state the positive outcomes of the open border policies
- State its implications on India's security
- Suggest way forward.

Answer:

Treaty of Peace and Friendship, 1950 facilitates free movement of people and goods between India and Nepal. Similarly, the India- Bhutan Friendship Treaty, 2007 has similar provisions. It is not mandatory for Indian citizens to have a visa to cross borders and vice-versa for the nationals of Nepal and Bhutan. Despite the presence of boundary demarcating pillars along the 699-km long Indo-Bhutan border and the 1,751km-long Indo-Nepal border, the border remains unfenced.

Benefits

- Enhanced cultural connectivity and tourism.
- Promotion of close ties between communities and border trade, thus promoting mutual gain.
- Efficient use of human capital: in Sikkim, Nepalese manpower has contributed significantly to the economic development of the area by providing seasonal agricultural labour.
- Strengthens diplomatic ties and helps India extend its soft power as Nepal and Bhutan are landlocked countries with small market and fewer economic opportunities.

Concerns

- Increased instances of human trafficking, smuggling of contraband goods, fake Indian currencies, arms and drugs.
- Guarding the open, porous international borders poses a challenge to the security forces. An open border allows easy egress to terrorists and insurgents. In the late 1980s, terrorist elements involved in Punjab and Kashmir sneaked into India via Nepal.
- Many insurgent groups from the North East, such as the United Liberation Front of Asom (ULFA), the National Democratic Front of Bodoland (NDFB), and the Kamtapur Liberation Organization (KLO), also misused the open border.
- Apart from insurgents and terrorists, many criminals pursued by Indian and Nepalese security forces escape across the open border.
- Inexpensive products made in China and elsewhere being supplied through this border.
- While all entry and exit points allow citizens of Nepal and Bhutan to enter India freely, there is no system to verify citizenship or registration of the people or vehicles entering through international entry points.

Measures such as identity check of people and vehicles crossing the borders and increased coordination with security forces of Bhutan and Nepal should be taken to address the emerging issues. Similarly, empowering and modernizing the Sashastra Seema Bal (SSB) guarding these borders is the need of the hour. Any decision about a change in the border administration should take into account the imperatives of Globalization and the interests of people on both side of the border.

10. Highlighting the role of space technology in border management, enumerate the steps taken so far in this regard.

Approach:

- Giving a brief scenario of difficulty in border management, discuss the role of space technology in border management in context of India.
- Enumerate the steps that have been taken in this regard.
- Highlight the various challenges associated with them.

- Conclude on the basis of the above points.

Answer:

India shares 15,200 km long land frontier with its surrounding countries, some of them being hostile neighbours like Pakistan and China. So, sealing the entire border becomes a major imperative. But variations in the terrain and topography are a huge challenge in achieving this task. So, utilising space technology is often touted as an effective way to overcome this challenge.

Role of space technology in border management:

- **Timely Information:** The information received through various satellites is used by various agencies including the security establishment. For instance, weather satellites can provide timely information about topographic features and weather conditions, which are critical to military and para-military operations.
- **Intelligence inputs and Surveillance:** Remote sensing satellites, radar satellites and satellites with synthetic aperture radar (SAR) sensors are capable of providing day and night all-terrain and all-weather inputs. Earth observation satellites provide detailed images of hot spots where border crossings peak. India uses the RISAT and Cartosat spacecraft to capture still images as well as high-resolution video of the nation's disputed borders.
- **Checking infiltration:** Deployment of Medium Altitude Long Endurance and High Altitude Long Endurance Unmanned Aerial Vehicles (UAVs), along with use of low orbit surveillance satellites can check infiltration and improve India's surveillance and reconnaissance capabilities
- **Coordination between agencies:** Border forces depend on intelligence shared by central agencies like IB, RAW and National Technical Research Organisation. They also face poor communication issues in areas like Ladakh, Sikkim, Arunachal Pradesh and Kashmir Valley. With satellite technology border security authorities can exchange information or access critical data from headquarters, border checkpoints or on the-move border patrol units.

Steps taken in this regard:

- A Space and Tech cell, within Home Ministry's Border Management Division is planned to be set-up to improve border management and help in operations.
- Navigation for use in border management by Indian Armed Forces is planned to be governed by indigenously developed NAVIC (IRNSS), reducing dependence on GPS.
- Communication: India has developed various satellites for communication purposes in military sphere, such as:
  - **GSAT-7 or INSAT-4F,** a multi-band military communications satellite developed by ISRO will enable Indian Navy to extend its blue water capabilities and stop relying on foreign satellites communication systems like Inmarsat.
  - **GSAT-7A,** which will augment Indian Air Force's existing satellite based communication capabilities.
- Satellite imagery for border management: The defense forces require specific scene-spot imagery according to the military's area of interest to help them track developments along India's land borders. The Cartosat series is made for this purpose itself. Similarly, Geo-Imaging Satellite (GISAT) will provide live, real-time images of large areas of India.

Also, **report of Task Force** created by Ministry of Home Affairs identifies areas of use of space technology in improving border management. Further such interventions should also address challenges like lack of effective deployment of manpower and non-timely execution of projects. Also, steps should be taken encourage private sector as well. Knowledge exchange and experience sharing with other countries should be stepped up as well

Heartiest Congratulations

to all Successful Candidates

8468022022 www.visionias.in

Aditya Srivastava

16 in **TOP 20** Selections in **CSE 2023**

from various programs of **Vision IAS**

Animesh Pradhan

Ruhani

Srishti Dabas

Anmol

Nausheen

Aishwaryam Prajapati

39 Selections in **TOP 50** in **CSE 2022**

Ishita Kishore

Garima Lohia

Uma Harathi N

SHUBHAM KUMAR

CIVIL SERVICES EXAMINATION 2020

HEAD OFFICE
Apsara Arcade, 1/8-B 1st Floor, Near Gate-6 Karol Bagh Metro Station
DELHI

MUKHERJEE NAGAR CENTER
Plot No. 857, Ground Floor, Mukherjee Nagar, Opposite Punjab & Sindh Bank, Mukherjee Nagar

GTB NAGAR CENTER
Classroom & Enquiry Office, above Gate No. 2, GTB Nagar Metro Building, Delhi - 110009

FOR DETAILED ENQUIRY
Please Call:
+91 8468022022,
+91 9019066066

enquiry@visionias.in /c/VisionIASdelhi /visionias.upsc /vision_ias VisionIAS_UPSC