## 1. With the internal security threats emanating from communication networks, what steps can be taken to regulate their misuse without violating the right to privacy and freedom of expression? Discuss.

### Approach

Candidates are expected to write about internal security threats emanating from the communications networks. And then suggests steps to regulate misuse.

### Introduction

In cutthroat competition and rapidly changing technical environment, there is more economic uncertainty and complexities that afflicting the nation. Security is described by experts as ensuring protected communication among computing/communication systems and user applications across public and private networks, is essential for guaranteeing confidentiality, privacy and data/information protection.

### Body

Recent issues threats emanating from the communication network –

- Various communication networks are the mainstay of much of the critical infrastructure in many sectors today such as civil aviation, shipping, railways, power, nuclear, oil and gas, finance, banking, IT, law enforcement, intelligence agencies, space, defence, and government networks.
- The Ministry of Home Affairs notification through its Cyber Coordination Center on ZOOM Application after Computer Emergency Response Team's (CERT-IN) raised concerns on video conferencing through the app in lockdown situation once again exposed the threats to the internal security through communication networks.
- 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. The whole incident brought forward the issue of digital security and the ways to achieve it with minimum loopholes.
- With the help of social media, people have started attacking each other's religion on this platform. Sensitive tweets regarding religion are becoming a common phenomenon. Circulation of certain pictures through communication networks also creates a panic among the masses. This is a threat to the internal security of the nation as it disturbs the communal harmony.
- Popular communication networks websites are another means of attracting potential members and followers. These types of virtual communities are growing increasingly popular all over the world, especially among younger

demographics. This can build Anti-national Sentiments among Society. Hackers write or use ready-made computer programs to attack the target computer. By using communication networks hackers breach the national security and steal important data of defence or other strategic sectors. This can kneel the whole country without using Arms and Ammunition.

Steps to regulate misuse without violating the fundamental rights –

- The National Informatics Centre (NIC) has launched an instant messaging platform called Sandes on the lines of WhatsApp. The National Informatics Centre (NIC) has launched an instant messaging platform called Sandes on the lines of WhatsApp.
- Governments across the world should strengthen their Cybersecurity Framework to deal with the threats posed by dark net. They must cooperate with each other regarding securing the Cyberspaces worldwide through intelligence, information, technology and expertise sharing.
- Real-time intelligence is required for preventing and containing cyber attacks. To achieve that, India needs to secure its computing environment and Internet of Things (IoT) with current tools, patches, updates and best-known methods in a timely manner.
- The need of the hour is to develop core skills in cyber-security, data integrity, and data security fields and setting up of stringent cyber-security standards to protect the institutional infrastructure of the country.
- The Ministry of Home Affairs has already taken effective measures to strengthen the national security apparatus and communication and information management systems. All internal security activities should be underpinned by vigorous information management to safeguard the effective use of resources and data assets.
- Nevertheless, security agencies face challenges at every stage of information management such as creation, collection, storage, and communication. To deal with such as challenges, security agencies must develop robust and automated information management and install various protective measures to protect from cyber threats.
- Development of Public Private Partnerships is an important strategy under the National Cyber Security Policy 2013. Pursuant to this aim, under the aforementioned Cyber Swachhta Kendra initiative, antivirus company Quick Heal is providing a free bot removal Tool.

## Conclusion

To summarize, internal security organisations in India and around the globe has to undergo unparalleled challenges such as the need to tackle crime, address the increasing challenge of Transnational criminal networks and the ongoing threat of international and domestic terrorism, cybercrime, money laundering, narcoterrorism and human trafficking.

## 2. Comment on the role played by media and social networking sites during the COVID pandemic.

### Approach

Candidate with the help of examples and anecdotes from the current happenings can give the picture of role played by traditional media and social media sites during the pandemic outlining positives and negatives of the platforms.

### Introduction

Human beings, from the history of their existence are connected like never before. Globalisation and communication revolution has drastically changed the way information is processed, received and spread. Covid-19 pandemic brought out some of the unique characteristics of this infodemic. Consistent information, misinformation and fake news have permanently changed the way we receive news.

### Body

The Covid-19 pandemic has caused social and economic disruptions all around the globe. Moreover, the worrisome situation is not just because of the pandemic but the ease at which fake news has been spreading around it. The World Health Organization (WHO) admitted that humanity is fighting two foes — a pandemic and an “infodemic”.

What is infodemic? Infodemic is an overabundance of information that makes it difficult for people to identify truthful and trustworthy sources from false or misleading ones. In the present state of emergency, a barrage of information on the virus has deluged the traditional and social media space.

Role of media and social networking sites during pandemic –

- As the cases of covid-19 is increasing day by day, the load of media to entertain people is also increasing. Here the role of Television and radio is very crucial, as most of the medium is not accessible. They are loaded with dual responsibility is not only entertaining the audience but also providing with relevant and genuine data.
- The initial role of media in this time or anytime is to educate, inform and entertain. And here the credibility arrives, things should be told with facts to avoid further conflict or confusion. It works as breeze between government and general public. Television has robust power to make how we see the world, as it so flexible that could influence the people in a large extent.
- The issues like tablighi jamaat were blown out of proportion by television media by calling it virus jihad. During the pandemic, sense of helplessness and polarisation was created among the sections of society. The role of

television media is to convey the information, with large graphics and loud announcements, media houses declared a kind of apocalypse is here.

- Even today we see glamorisation of poverty and sufferings of common man, media should be sensitive enough to understand the sufferings of patients and their relatives and choose not to go after sensationalization.

Social networking sites –

- Social Media, with its ability to amplify a message through endorsements and forwards, gives one the tool to reach a potential audience without needing substantial resources or access to expensive media technology.
- Social media provides the tools for an information cascade. It enables individuals to distribute large volumes of disinformation or fake news. Today's decision-making is not based on individual rationality but from shared group-level narratives. Social media helps in making the false and misleading narratives of some social miscreants.
- There are rising dangerous conspiracy theories of Covid-19 of being a Bioweapon. A rumour of a lockdown of essential commodities resulted in people hoarding the essential supplies.
- Social media did played positive role as a crucial conduit between families, friends, office, and a medium of entertainment. A reliable way for the victims of this virus to communicate with the outside world.
- In response to Covid-19 pandemic, it gave birth to a fair share of online fundraisers. For example, donations in the PM-CARES fund got encouraged by people sharing this on social media.
- People are also giving money to financially struggling hospitals, as well as individuals at risk of dying from the disease. From plasma to oxygen cylinders, information is disseminated through social media.
- Social media displays and strengthens solidarity against this virus. For example, Indian Prime Minister called for lighting lamps to reinforce the public commitment to fight Covid-19.
- WHO and other public health organizations also use social media to inform the public about the outbreak, and control the panic. It is being used to spread preventive steps that one can take to fight Covid-19. These small changes in behaviours can have enormous consequences.

## Conclusion

Traditional media and in particular social media is a two edged sword. Fake information spreads faster than the virus and it mutates with an enormous speed. To immune ourselves from this virus of misinformation we have to take vaccine of optimum use of social media platforms and be informed from the authentic media platforms and not to run after the sensationalization.

## 3. Why is fake news considered a serious internal security threat? Analyse.

### Approach

Since the question is asking you to analyse, you are expected to break an issue into constituent parts and explain how these relate to one other and present as one summary.

### Introduction

The word 'Fake News'- Word of the Year, 2017 by Collins Dictionary got popularised in the 2016 US Presidential election and Brexit. It is much debated in communication fields and social sciences as it has the potential to polarise public opinion, to incite violence and extremism.

### Body

**WHY FAKE NEWS IS CONSIDERED A SERIOUS INTERNAL SECURITY THREAT?**

- Fake news has the potential to polarise public opinion, to promote violent extremism and hate speech and, ultimately, to undermine democracies and reduce trust in the democratic processes.
- The countries which are already suffering from ethnic tensions, misinformation can exasperate a lot of tensions and can also generate violence.
- Rumours spread through fake news can create a lot of social turmoil in a country or among the countries.
- In perhaps, the well-known case, Myanmar during the Rohingya crises Facebook was used as a tool or weapon by the people to incite violence against the Rohingya Muslims.
- Buddhists were influenced by the rumors which led them to target Muslims. To retaliate the harm caused on Muslim in Myanmar, Indian Muslim attack Bodh Gaya temple of India.
- In India, rumors spread by Whatsapp led to many communal riots. Riot in Muzaffarnagar in 2013 where around 50 people were killed is the example of one such case out of many which takes place every year.
- Jammu & Kashmir witnessed internet shutdowns quite in high frequency after any military operation takes place or after any act related to the state, which is of sensitive nature, is passed by the legislature in order to restrict the circulation of fake news and misinformation which can make situation worst.
- Across the country, there is a rise in numbers of mob attacks fueled by rumors spread by using social media handles like Whatsapp, Facebook, twitter etc.

- Fake news, state-funded disinformation and propaganda directly challenge the question of national security and the democratic set-up of any nation. The whole system and set-up have turned into more complicated and complex state, and the challenges that it present cannot be met by mere simple solutions; they require open, deep and critical analysis.

## Conclusion

Fake news and disinformation are definitely a threat to a nation's security both externally as well as internally. There is need of codified rules in order to check the authenticity and reason of arrest of rumor-monger by official. Online platform, social media or other such private companies that act as a platform to communicate, too has desired role to play in this process of curbing fake news. It is their responsibility to check the validity of information and disclose the details creator before passing liability to government to do the same. It is a responsibility of every individual to combat the scourge of fake news. It can include improving digital literacy among the general public and supporting investigative journalism.

## 4. What are the security challenges posed by emerging technologies like artificial Intelligence and block chain? Discuss.

### Approach

Question is straight forward in its approach students are expected to write about the security challenges posed by emerging technologies like artificial intelligence and blockchain technology also it is important to substantiate with examples as well.

### Introduction

Artificial intelligence and block chain are the new disruptive technologies emerging across sectors worldwide Artificial Intelligence (AI) is fast evolving as the go-to technology for companies across the world to personalise experience for individuals. The technology itself is getting better and smarter day by day, allowing more and newer industries to adopt the AI and blockchain for various applications. The rudimentary applications AI include bring smarter chat-bots for customer service, personalising services for individuals, and even placing an AI robot for self-service at banks. Beyond these basic applications, banks can implement the technology for bringing in more efficiency to their back-office and even reduce fraud and security risks.

### Body

**Security challenges posed by Artificial Intelligence and block chain are as follows –**

- Hackers are embracing the machine learning algorithms behind the technology's success to create nuanced attacks personalized for specific individuals. Because AI can be "taught" with data sets, hackers can either create their own programs or manipulate existing systems for malicious purposes. Attacks executed with AI tend to be more successful, perhaps because the technology makes it easier to develop malware with the ability to evade even sophisticated threat detection. For example, pairing polymorphic malware with AI allows these programs to change their code rapidly, making them almost invulnerable to existing cybersecurity systems.
- Massive Data Centres Needed – Achieving the abovementioned objectives, AI requires massive computational capacity, which means more power-hungry data centres and a big carbon footprint.
- Jurisdictional Issues of Data Pooling – Countries are passing stricter legislations on data security (E.g. EUGDPR) that require citizen data to be stored on servers located domestically, picking colder climates beyond their borders is becoming a difficult option.
- The increasing accessibility of facial-recognition technology has also increased concerns with respect to privacy, security, and civil liberties.
- Data immutability has always been one of the biggest disadvantages of the blockchain. It is clear that multiple systems benefit from it including supply

chain, financial systems, and so on. However, if you take how networks work, you should understand that this immutability can only be present if the network nodes are distributed fairly.

- Another problem that it suffers from is the data once written cannot be removed. Every person on the earth has the right to privacy. However, if the same person utilizes a digital platform that runs on blockchain technology, then he will be unable to remove its trace from the system when he doesn't want it there. In simple words, there is no way he can remove his trace, leaving privacy rights into pieces.
- 51% attack is sometimes so critical that the intruders can gain control over the system for sure. Such a network will be affected by double-spending too. The security threat is aggravated by the anonymous nature of this bitcoin system. Anonymity is appreciated, but identifying culprits attempting illicit transactions is difficult here. Less Transparency is a downside of blockchain technology so far.
- In blockchain technology, it is hard to add or modify data once after it is recorded. It is considered as the major disadvantages and advantages of blockchain technology. Considering its downside, the process of data modification needs rewriting codes and indulges in an extensive process. Too much stability can sometimes adversely affect systems. The major disadvantage of blockchain technology here is irreversible records and its demanding modification process.

## Conclusion

Blockchain technology and Artificial intelligence has proven itself robust and secure. It ensures integrity of the data and reduces incidents of fraud. The decentralised nature of the blockchain technology applications makes it a perfect fit for many industries to carry out secure business transactions. The proper use of blockchain technology allows us to avoid the use of middlemen or partner platforms in a peer-to-peer network, reduce reception time, fraudulent proof. Similarly Artificial Intelligence has a promising future and has everything for the benefit of humankind if concerns regarding security are alleviated fully.

## 5. What are the most common international destinations used for money laundering? What measures have been taken to control it?

### Approach

The candidate needs to elaborate upon the most common international destinations used for money laundering in the first part of the answer while in the second part, one needs to show some measures taken to control it.

### Introduction

Money laundering is the processing of criminal proceeds to disguise their illegal origin. It is the concealing or disguising identity of illegally obtained proceeds so that they appear to have originated from legitimate sources. It is frequently a component of other, much more serious, crimes such as drug trafficking, robbery or extortion. According to the IMF, global Money Laundering is estimated between 2 to 5% of World GDP.

### Body

- As money laundering is a consequence of almost all profit generating crime, it can occur practically anywhere in the world. Generally, money launderers tend to seek out countries or sectors in which there is a low risk of detection due to weak or ineffective anti-money laundering programmes.
- Money laundering activity may also be concentrated geographically according to the stage the laundered funds have reached. At the placement stage, for example, the funds are usually processed relatively close to the under-lying activity.
- With the layering phase, the launderer might choose an offshore financial centre, a large regional business centre, or a world banking centre – any location that provides an adequate financial or business infrastructure.
- Finally, at the integration phase, launderers might choose to invest laundered funds in still other locations if they were generated in unstable economies or locations offering limited investment opportunities.
- Currently, The Financial Action Task Force (FATF) has 'call for actions' in Iran and Dem. Rep Korea. These countries are considered very high risk and are not members of any anti-money laundering (AML) organisations, meaning no laws are in place to help combat money laundering.
- According to the Basel anti-money laundering index, the top 10 countries currently facing the greatest risk of money laundering are – Afghanistan (8.16), Haiti (8.15), Myanmar (7.86), Laos (7.82), Mozambique (7.82), Cayman Islands (7.64), Sierra Leone (7.51), Senegal (7.30), Kenya (7.18), and Yemen (7.12).

Steps Taken to Prevent Money Laundering –

- **The Vienna Convention:** It creates an obligation for signatory states to criminalize the laundering of money from drug trafficking.
- **The United Nations office on Drugs and Crime:** It proactively tries to identify and stop Money Laundering.
- **The Financial Action Task Force:** It has been set up by the governments of the G-7 countries at their 1989 Economic Summit, has representatives from around the world. It monitors members' progress in applying measures to counter Money Laundering.
- **India** is a full-fledged member of the FATF and follows the guidelines of the same. Further, Financial Intelligence Unit-IND is an independent body reporting directly to the Economic Intelligence Council (EIC) headed by the Finance Minister.
- **Criminal Law Amendment Ordinance (XXXVIII of 1944):** It covers proceeds of only certain crimes such corruption, breach of trust and cheating and not all the crimes under the Indian Penal Code.
- **The Smugglers and Foreign Exchange Manipulators (Forfeiture of Property) Act, 1976:** It covers penalty of illegally acquired properties of smugglers and foreign exchange manipulators and for matters connected therewith and incidental thereto.
- **Narcotic Drugs and Psychotropic Substances Act, 1985:** It provides for the penalty of property derived from, or used in illegal traffic in narcotic drugs.
- **Prevention of Money-Laundering Act, 2002 (PMLA):** It forms the core of the legal framework put in place by India to combat Money Laundering. The provisions of this act are applicable to all financial institutions, banks (Including RBI), mutual funds, insurance companies, and their financial intermediaries.
- **PMLA (Amendment) Act, 2012:** Adds the concept of 'reporting entity' which would include a banking company, financial institution, intermediary etc. It has provided for provisional attachment and confiscation of property of any person involved in such activities.
- **Enforcement Directorate (ED):** It is a law enforcement agency and economic intelligence agency responsible for enforcing economic laws and fighting economic crime in India.

## Conclusion

In addition to creating laws that criminalize the laundering of the proceeds of crime, India must also enact strict compliance programs for the financial industry that make it more difficult to launder money. India must negotiate additional Mutual Legal Assistance Treaties with other countries. MLATs are invaluable to international judicial assistance. If India intends to curb its escalating drug problem, it must take an aggressive stance with respect to money laundering.