1. The vision of tapping the potential of India's massive digital transformation must be balanced with a strategy to counter the associated security threats. Elucidate.

Approach

Candidates need to write about the digital transformation in India and with increased digital penetration write about the associated threats and suggest strategy to tackle such threats.

Introduction

Towards vision of tapping the digital transformation, India already is the 2nd largest online market worldwide. Although the advancement of technology and the internet has brought with it all related benefits but has also led to an increase in the cybercrime affecting and vulnerability of India to cyber-crime threats is more.

Body

Threats with digital transformation:

- Low end use digital financial education: With limited awareness about digital financial service, person is always vulnerable to external threats.
- Phishing: is the fraudulent attempt to obtain sensitive information such as usernames, and passwords.
- Cyber terrorism: premeditated, politically motivated attack against information, computer systems and data which results in violence.
- Pishing/Social engineering: Vishing works like phishing but does not always occur over the Internet and is carried out using voice technology.
- Hacking: Hackers intrude into others financial domains and make financial transactions into their digital accounts.
- Cyber Ransom: Ransomware is a form of malware that encrypts a victim's files. The attacker then demands a ransom from the victim to restore access to the data upon payment.
- Ineffective firewall system: This can be ineffective in tackling the virus/corrupt files with an intent to collect crucial information.
- DDoS Attack: It is a malicious attempt to disrupt normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure.
- Unregulated Cryptocurrency: Any cyber-attack (Crypto-Jacking) on such financial transactions can be a potential threat with no regulations available.

Strategy to counter the security threats:

- R&D: Investments should be made on R&D to develop more innovative technologies to address increasing cyber security threats.
- Awareness: A periodic awareness campaign by the government and big private organizations should be conducted to aware people about cyber security threats.
- Strengthening Private Partnership: It is important to strengthen the public-private partnership on cyber security.
- Policy and Governance: Further, duties and responsibilities should be defined clearly for smooth functioning and better coordination among departments and stakeholders.
- India should become signatory to cybercrime convention (Budapest Convention) which puts a hurdle in dealing with transborder crime particularly.

Conclusion

With estimates of India creating $1 trillion of economic value from the digital economy by 2025. India should not loose on the cyber-attack front. Government and the private sector jointly have to give cyber security some priority in their security and risk management plan.

2. The role of media has changed in recent years. There is an acute dearth of independent and unbiased journalism. What makes the situation worse is the rampant misuse of media to polarise the society. Comment.

Approach

Students are expected to give basic information on role of media and then comment on changing role of media with advent of new age social media and different apps. How it created yellow journalism and polarised the situation.

Introduction

The role of the media is vital as a watchdog for uncovering errors and wrongdoings in the democracy. Media provides the platform for people tend to discuss & debate news over any topics. This interaction of people from varied backgrounds strengthens civil engagement in society.

Body

Changing role of media:

- Fake news: Fake news is not a new phenomenon which is linked to the rise of social media. The emerging threat of fake news could have an unprecedented impact on election cycle, raising serious questions about the integrity of democratic elections, policy-making and our society at large.
- Use of tech: Computational propaganda is the use of algorithms, automation, and human curation to purposefully distribute misleading information over social media networks.
- Unable to balance competing interests: Media companies have been unable to balance the national security concerns with the capitalist motivations of profit.
- Half-baked Opinions: Media anchors for increasing viewership can comment on law and order and national security matters without responsibility.
- Intolerance to Contrary views: One of the most common criticisms of embedded journalism or media is that it creates echo chambers where people only see viewpoints they agree with further driving us apart for polarization.

Making situation worse:

- With the advent of social media, technological changes, the reach of media has grown profoundly. Its reach and role in impacting public opinion have made it even more important worse.
- The sensationalism-driven reporting compromised the identities of rape victims and survivors despite SC guidelines.
- Fake news, yellow journalism are important concerns which are influencing public and impacting national security. For instance, fear mongering through media has led to mob lynchings, attacks on the migrant population.

Conclusion

In developing countries like India, the media have a great responsibility to fight backward ideas such as casteism and communalism and help the people in their struggle against poverty and other social evils. Hence, having journalistic ethics in place becomes very important.

3. Discuss the security threats emanating from money laundering activities. What steps have been taken by the government to check money laundering? Discuss.

Approach-

Candidates need to explain the security threats emanating from money laundering activities. Also mention the steps taken by the government to check money laundering.

Introduction:

India is extensively gripped under crime of money laundering. Money laundering is usually used by criminals to hide money made through illegal act. It is the process by which huge amount of money obtained unlawfully, from drug trafficking, terrorist activity or other severe crimes. India is among the high-risk areas for money laundering. Therefore, the Indian government needs to take Anti-Money Laundering measures together with their developing economies.

The security threats emanating from money laundering activities.

- Even though the use of emerging technologies like artificial intelligence, machine learning, and big data for countering financial crimes, insufficient anti-money laundering systems are contributing to increasing money laundering and terrorist financing activities.
- As we navigate through the debate on crypto's future in India, mere imposing a 30 per cent tax on digital assets is not enough as money laundering and hawala-based transactions are growing significantly via cryptocurrencies on the Dark Web, putting India's national security at risk.
- Grave concerns are there over the misuse of digital coins on the Dark Web for terror acts and drugs trafficking by militant organisations, and for money laundering and hawala-based transactions — posing a serious threat to national security and a big challenge to the security agencies in the country.
- We have to realise that if we do not take effective appropriate steps fast, this crypto-based tech is going to be extensively used by terrorists for the purpose of targeting the sovereignty, security and integrity of India.

Steps taken by the government to check money laundering

- Governments have taken specific measures in the past to prevent money laundering. The purpose of these measures is to prevent financial crimes and ensure the administrative and economic stability of the country.
- The governments of India aim to protect the country from money laundering risks through laws and legal mechanisms.
- India enacted the Prevention of Money Laundering Act in 2002.
- The laws and regulations prior to this law were insufficient to combat money laundering.
- The Prevention of Money Laundering Act has entered into force to combat money laundering and prevent money laundering.
- The money laundering crime in India has huge penalties. According to AML laws in India, people committing money laundering offenses are sentenced to up to 10 years in prison.
- The Financial Intelligence Unit of India (FIU-IND) is the organization responsible for the fight against the financial crimes of India under the

Ministry of Finance. Businesses with AML obligations report to the Financial Intelligence Unit.

- RBI also has some regulatory powers to prevent money laundering.
- In addition, India is among the countries that are members of FATF. FATF is a global organization established to prevent money laundering all over the world.
- By publishing AML guidelines, FATF aims for countries to fight financial crime more effectively. The FATF member states' AML regimes must comply with FATF recommendations.

Conclusion

There is a lot to consider regarding AML trends and typologies. The fight against money laundering and cybercrime has been an arms race since the dawn of the internet. Failure to take the necessary measures increases money laundering crimes in India and undermines India's reputation in the international arena. Now more than ever, it's essential to stay up to date.