Defence & Security · GS - III

Social media and encrypting messaging services pose a serious security challenge. What measures have been adopted at various levels to address the security implications of social media? Also suggest any other remedies to address the problem.

EXAM YEAR	PAPER	SUBJECT
2024	GS - III	Defence & Security

MARKS	WORD LIMIT
15	~250 words

Answer Hint

Social media, encrypted messaging, misinformation, cybercrime, national security, intermediary liability, IT Rules 2021, traceability, CERT-In, cyber awareness, encryption-security balance

Model Answer

Introduction

Social media and encrypted messaging platforms have transformed communication but can also facilitate misinformation, cybercrime, radicalisation, fraud, coordinated violence and anonymous dissemination of harmful content. India has consequently developed a multi-layered regulatory and institutional response.

Body

1. Measures Adopted

Legal and regulatory framework: The Information Technology Act, 2000 and the **Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021** establish due-diligence obligations for intermediaries and mechanisms for grievance redressal.

Greater accountability of significant platforms: Significant social-media intermediaries have additional compliance obligations, including designated grievance and compliance mechanisms.

Cybersecurity institutions: CERT-In coordinates responses to cyber incidents and issues directions relating to cybersecurity practices and incident reporting.

Law-enforcement action: Police and specialised cybercrime units investigate online fraud, extremist propaganda, threats and other digital offences.

International cooperation: Cybercrime increasingly requires cooperation with foreign governments and technology platforms because digital evidence frequently crosses jurisdictions.

2. Further Remedies

- Develop stronger cyber-forensics and digital-evidence capabilities.
- Improve intelligence sharing between central agencies, State police and platforms.
- Promote cyber literacy and responsible digital behaviour.
- Establish rapid mechanisms for reporting and removing demonstrably unlawful content while protecting lawful expression.
- Strengthen platform transparency, independent audits and algorithmic accountability.
- Use privacy-preserving technologies while addressing legitimate security requirements.
- Strengthen cooperation against cross-border cybercrime.

Conclusion

The objective should not be unrestricted surveillance but a balanced framework that protects **national security, privacy, encryption, freedom of expression and rule of law**. Technology, institutional capacity and citizen awareness must therefore operate together.

BECOME IAS
AI POWERED UPSC PREP