Defence & Security · GS - III

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.

EXAM YEAR	PAPER	SUBJECT
2016	GS - III	Defence & Security

MARKS	WORD LIMIT
12.5	~200 words

Answer Hint

Cybersecurity; online radicalisation; misinformation; encrypted communication; cybercrime; digital forensics; platform accountability; freedom of expression

Model Answer

Introduction

Internet platforms and social media facilitate communication and public participation, but non-state actors can also exploit them for radicalisation, disinformation, cybercrime and activities that threaten public order and national security.

Forms of Misuse

- **Radicalisation and recruitment:** Extremist networks distribute propaganda, identify vulnerable users and encourage support for violent causes.
- **Misinformation:** False or manipulated content can provoke communal tension, panic or violence.
- **Coordination of unlawful activity:** Online groups may use digital channels to coordinate disruptive actions or evade detection.

- **Cyberattacks:** Criminal and hostile actors may target government systems, critical infrastructure and private networks.
- **Fundraising and fraud:** Online payment channels, deceptive campaigns and illicit digital transactions may support criminal or extremist networks.
- **Data exploitation:** Stolen personal information can facilitate intimidation, impersonation and targeted manipulation.

Effective Guidelines to Curb the Threat

1. Stronger Cybersecurity

Improve threat monitoring, incident response, digital forensics and protection of critical information infrastructure.

2. Platform Accountability

Require lawful and proportionate action against illegal content, transparent reporting and timely cooperation with authorised investigations.

3. Public Awareness

Promote digital literacy, verification of information, safe online behaviour and reporting of suspicious activity.

4. Financial Disruption

Strengthen monitoring of suspicious transactions and cooperation among financial institutions and law-enforcement agencies.

5. Inter-agency Coordination

Improve information-sharing between cybersecurity bodies, police, intelligence agencies and relevant international partners.

6. Legal Safeguards

Apply clear legal standards, due process and independent oversight. Restrictions should be necessary and proportionate, protecting legitimate expression and privacy.

Conclusion

Combating online subversion requires technological capability, platform cooperation, public awareness and international coordination. Security measures must remain consistent with constitutional rights and the rule of law.