Defence & Security · GS - III

Cyber espionage and honey-trapping pose emerging threats to India's defence establishments. Examine the challenges and suggest measures to strengthen national security.

EXAM YEAR	PAPER	SUBJECT
DAILY PRACTICE 23/10/2026	GS - III	Defence & Security

MARKS	WORD LIMIT
10	~150 words

Answer Hint

Cyber warfare, social engineering, counter-intelligence, defence cybersecurity, personnel awareness, CERT-In, information security.

Model Answer

Introduction:

Cyber espionage involves covertly obtaining sensitive information through digital means. When combined with honey-trapping, it can expose military personnel and defence establishments to serious security risks.

Main Body

Major Challenges

1. Human vulnerability: Emotional manipulation and fake online identities can compromise personnel.
2. Technical threats: Phishing, spyware and malicious applications can steal confidential data.
3. Insider threats: Individuals with legitimate access may deliberately or unknowingly disclose sensitive information.

4. Attribution difficulties: Foreign operators can conceal their identities through encrypted communications and intermediaries.

Way Forward

- Strengthen firewalls, endpoint security, encryption and multi-factor authentication.
- Conduct regular cybersecurity and counter-intelligence training for defence personnel.
- Enforce strict protocols for handling classified information and using personal devices.
- Improve coordination among military intelligence, CERT-In and law-enforcement agencies.
- Establish prompt reporting mechanisms and conduct regular security audits.
-

Conclusion:

India needs an integrated approach combining advanced technology, personnel awareness and effective counter-intelligence. Protecting sensitive defence information is essential to safeguarding operational readiness and national security.

BECOME IAS
AI POWERED UPSC PREP