Defence & Security · GS - III

Insider threats and social engineering have expanded the scope of national security beyond conventional espionage. Discuss the challenges they pose to India's defence establishments and suggest a comprehensive framework for strengthening counter-intelligence and institutional security.

EXAM YEAR	PAPER	SUBJECT
DAILY PRACTICE 16/11/2026	GS - III	Defence & Security

MARKS	WORD LIMIT
10	~150 words

Answer Hint

Insider threats, honey trapping, social engineering, counter-intelligence, cyber espionage, personnel vetting, classified information, CERT-In, NTRO, security awareness, zero-trust architecture, inter-agency coordination, accountability.

Model Answer

Introduction

National security increasingly depends on protecting sensitive information, digital infrastructure and institutional personnel. Insider threats exploit legitimate access, while social engineering manipulates individuals to obtain confidential information.

Major Security Challenges

1. **Human vulnerabilities:** Honey trapping, blackmail, impersonation and financial inducements can compromise personnel with access to classified information.

2. **Cyber espionage:** Phishing, malware and credential theft can provide foreign intelligence actors access to sensitive networks.
3. **Insider access:** Employees or contractors may misuse authorised access, intentionally or negligently.
4. **Technological complexity:** Cloud systems, remote access and interconnected defence networks expand potential vulnerabilities.
5. **Detection difficulties:** Malicious activities may appear similar to legitimate communication or routine data access.

Measures to Strengthen Security

- **Personnel security:** Periodic background verification, risk-based access controls and continuous security awareness.
- **Cyber resilience:** Multi-factor authentication, encryption, network segmentation and zero-trust architecture.
- **Institutional vigilance:** Strong counter-intelligence mechanisms, confidential reporting channels and regular security audits.
- **Inter-agency coordination:** Better information sharing among defence intelligence organisations, NTRO and cyber security agencies.
- **Accountability:** Clear protocols for handling classified information and prompt investigation of security breaches.

Conclusion

Effective defence security requires integrating technological safeguards with personnel vigilance and institutional accountability. A proactive counter-intelligence framework is essential to protect India's strategic capabilities.

BECOME IAS
AI POWERED UPSC PREP