Defence & Security · GS - III

Critically examine the vulnerabilities arising from the use of informal digital communication networks by personnel in India's defence establishment.

EXAM YEAR	PAPER	SUBJECT
DAILY PRACTICE 25/11/2026	GS - III	Defence & Security

MARKS	WORD LIMIT
15	~250 words

Answer Hint

Digital infiltration, social engineering, operational security, insider threats, cybersecurity protocols, institutional accountability

Model Answer

Digital communication has improved coordination and connectivity, but the use of unofficial messaging groups by defence personnel can create serious vulnerabilities in a security-sensitive environment.

Nature of the vulnerabilities

1. **Identity compromise:** Attackers using compromised phone numbers or impersonated identities can enter groups and gain access to internal conversations.
2. **Social engineering:** Personnel may unknowingly disclose deployment details, operational routines or sensitive documents through apparently trustworthy interactions.
3. **Metadata exposure:** Even without accessing message contents, information about communication patterns, contacts and timings can reveal organisational relationships.
4. **Information leakage:** Forwarding screenshots, photographs and documents can expose sensitive information beyond the intended audience.
5. **Insider threats:** Negligence, weak authentication or deliberate disclosure can compromise operational security.

Institutional implications

Such vulnerabilities can expose troop movements, weaken operational preparedness and undermine confidence in secure communication systems. They also demonstrate that cybersecurity is not merely a technological issue but a matter of personnel discipline and institutional governance.

Strengthening the security framework

1. Establish mandatory audits of unofficial communication groups and remove unauthorised participants.
2. Enforce clear restrictions on sharing official information through personal messaging applications.
3. Provide secure, authenticated communication platforms for authorised personnel.
4. Conduct regular cybersecurity training, phishing simulations and incident-response exercises.

India must adopt a layered security approach combining technological safeguards, personnel awareness and enforceable protocols. **A strong defence cybersecurity framework must treat human behaviour as an integral component of national security.**

BECOME IAS
AI POWERED UPSC PREP