Defence & Security · GS - III

The growing convergence of cyber espionage, artificial intelligence and supply-chain vulnerabilities has expanded the threat landscape for national security. Examine the measures required to protect India's strategic defence and technology ecosystem.

EXAM YEAR	PAPER	SUBJECT
DAILY PRACTICE 19/11/2026	GS - III	Defence & Security

MARKS	WORD LIMIT
15	~250 words

Answer Hint

Cyber espionage, defence technology, critical information infrastructure, supply-chain security, AI-enabled threats, counter-intelligence, CERT-In, NCIIPC, public-private partnership, international cooperation

Model Answer

Introduction

National security increasingly depends on protecting sensitive digital infrastructure, intellectual property and defence technologies. Cyber espionage and supply-chain attacks can compromise strategic capabilities without conventional military confrontation.

Emerging Threats

1. **Cyber espionage:** Foreign intelligence networks may target defence personnel, research institutions and technology companies to obtain classified information.
2. **Supply-chain vulnerabilities:** Compromised software, hardware or third-party vendors can provide indirect access to sensitive networks.

3. **AI-enabled intrusions:** Artificial intelligence can enhance phishing, automate vulnerability discovery and support sophisticated cyber operations.
4. **Insider threats:** Employees with legitimate access may intentionally or unintentionally expose confidential information.
5. **Intellectual property theft:** Stolen research and defence innovations can weaken India's technological and strategic advantage.

Measures Required

- **Institutional strengthening:** Enhance the capabilities of CERT-In and the National Critical Information Infrastructure Protection Centre (NCIIPC).
- **Zero-trust security:** Adopt continuous authentication, restricted access privileges and multi-factor authentication.
- **Supply-chain audits:** Screen vendors, verify software integrity and conduct regular security assessments.
- **Counter-intelligence:** Strengthen personnel verification, threat monitoring and intelligence coordination.
- **Indigenous capabilities:** Promote domestic cybersecurity technologies and secure defence research ecosystems.
- **International cooperation:** Develop information-sharing mechanisms and collaborative responses to cross-border cyber threats.

Conclusion

Protecting strategic technologies requires an integrated approach combining cybersecurity, counter-intelligence, institutional accountability and technological self-reliance. Cyber resilience must become an essential component of India's national security architecture.