Science & Technology · GS - III

Assess the significance of cybersecurity resilience in protecting critical government information infrastructure against increasingly sophisticated cyber threats.

EXAM YEAR	PAPER	SUBJECT
DAILY PRACTICE 25/11/2026	GS - III	Science & Technology

MARKS	WORD LIMIT
15	~250 words

Answer Hint

Cyber espionage, critical information infrastructure, defence-in-depth, zero-trust architecture, data protection, institutional coordination, incident response

Model Answer

Introduction

Government institutions increasingly depend on digital networks for intelligence, administration and strategic decision-making. Cyberattacks targeting even unclassified systems can expose operational information, compromise institutional credibility and provide entry points for further intrusion.

Significance of Cybersecurity Resilience

1. **National security:** Protection of government networks reduces the risks of cyber espionage, intelligence theft and disruption of strategic operations.

2. **Administrative continuity:** Secure digital infrastructure ensures uninterrupted delivery of essential public services during cyber incidents.

3. **Protection of sensitive information:** Unclassified information may still reveal institutional procedures, personnel details and operational patterns that can be exploited by hostile actors.

4. **Strategic autonomy:** Strong domestic cybersecurity capabilities reduce dependence on external technologies and strengthen national control over critical digital assets.

Major Vulnerabilities

1. **Human factors:** Phishing, weak passwords and insider threats frequently compromise organisational security.

2. **Legacy infrastructure:** Outdated software and poorly secured networks create exploitable vulnerabilities.

3. **Fragmented coordination:** Inadequate information-sharing between agencies delays threat detection and response.

Way Forward

1. **Defence-in-depth:** Adopt network segmentation, encryption, multi-factor authentication and continuous security monitoring.

2. **Zero-trust architecture:** Verify every access request and follow the principle of least privilege.

3. **Institutional preparedness:** Conduct regular security audits, penetration testing and cyber-response exercises.

4. **National coordination:** Strengthen cooperation among CERT-In, the National Critical Information Infrastructure Protection Centre (NCIIPC) and relevant government agencies.

Conclusion

Cybersecurity is an essential component of national security and digital governance. India must move beyond reactive protection towards a resilient, continuously monitored and institutionally coordinated cybersecurity ecosystem.

BECOME IAS
AI POWERED UPSC PREP