Science & Technology · GS - III

Increasing dependence on interconnected digital infrastructure and centralised cloud services has created new systemic vulnerabilities. Analyse the implications of technological complexity for India's critical infrastructure security and suggest measures to strengthen resilience.

EXAM YEAR	PAPER	SUBJECT
DAILY PRACTICE 20/11/2026	GS - III	Science & Technology

MARKS	WORD LIMIT
15	~250 words

Answer Hint

Digital interdependence, cloud concentration, single points of failure, critical information infrastructure, cyber resilience, AI dependence, redundancy, decentralisation, disaster recovery, public-private partnership.

Model Answer

Introduction

Digital technologies have improved efficiency, connectivity and service delivery. However, growing dependence on interconnected systems, centralised cloud platforms and artificial intelligence creates systemic risks, where failure in one component can disrupt multiple essential services.

Implications of Technological Complexity

1. **Cascading failures:** Disruption in a major cloud provider or software platform can affect aviation, banking, healthcare and government services simultaneously.

2. **Single points of failure:** Excessive dependence on a limited number of technology providers creates concentration risks.
3. **Cybersecurity threats:** Greater connectivity expands the attack surface for ransomware, supply-chain attacks and unauthorised access.
4. **Operational dependence:** Automation may weaken manual capabilities and institutional preparedness during technological outages.
5. **Strategic vulnerability:** Dependence on foreign technology providers can raise concerns regarding data sovereignty and national security.

Measures to Strengthen Resilience

- **Redundancy and diversification:** Avoid excessive dependence on a single cloud provider through multi-cloud and alternative infrastructure arrangements.
- **Business continuity:** Maintain offline procedures, manual backups and regularly tested disaster-recovery systems.
- **Cybersecurity governance:** Strengthen security audits, incident reporting and supply-chain risk assessments.
- **Institutional coordination:** Improve coordination among CERT-In, NCIIPC, sectoral regulators and critical infrastructure operators.
- **Responsible AI adoption:** Conduct risk assessments before deploying AI in essential public services.
- **Regular simulation exercises:** Test infrastructure against cyberattacks, power failures and communication disruptions.

Conclusion

Technological progress must be accompanied by resilience, redundancy and accountability. India's digital transformation should prioritise systems that remain functional during disruptions rather than pursuing efficiency through excessive centralisation alone.

BECOME IAS
AI POWERED UPSC PREP