Defence & Security · GS - III

Keeping in view India’s internal security, analyse the impact of cross-border cyber attacks. Also discuss defensive measures against these sophisticated attacks.

EXAM YEAR	PAPER	SUBJECT
2021	GS - III	Defence & Security

MARKS	WORD LIMIT
10	~150 words

Answer Hint

Critical information infrastructure, cyber espionage, financial fraud, ransomware, power-grid threats, defence networks, data theft, state-sponsored actors, CERT-In, National Critical Information Infrastructure Protection Centre, cyber resilience, international cooperation

Model Answer

Introduction

Cross-border cyber attacks use digital networks to disrupt, infiltrate or steal information from systems located in another country. They pose growing risks to India's national security and economic stability.

Impact on India's Internal Security

- **Critical infrastructure:** Attacks on electricity, telecommunications, transport and financial networks can disrupt essential services.
- **Defence and espionage:** Intrusions into military and government systems may expose sensitive information and operational plans.
- **Economic damage:** Ransomware, banking fraud and attacks on businesses cause financial losses and undermine confidence.

- **Social instability:** Disinformation campaigns and coordinated online manipulation can inflame communal tensions.
- **Strategic coercion:** State-sponsored attacks may weaken India's preparedness while allowing perpetrators to operate across borders with plausible deniability.

Defensive Measures

- Strengthen the Indian Computer Emergency Response Team (CERT-In) and the National Critical Information Infrastructure Protection Centre (NCIIPC).
- Conduct regular security audits, vulnerability assessments and penetration testing.
- Adopt multi-factor authentication, encryption, secure backups and zero-trust access controls.
- Improve real-time threat intelligence sharing among government, defence agencies and private operators.
- Develop indigenous cyber capabilities, skilled personnel and incident-response exercises.
- Strengthen international cooperation, cybercrime investigations and diplomatic mechanisms.

Conclusion

India needs a whole-of-nation cyber-security framework combining prevention, rapid detection, coordinated response and resilient recovery. Protecting critical infrastructure must be treated as a core internal-security priority.

BECOME IAS
AI POWERED UPSC PREP