Science & Technology · GS - III

Examine the challenges posed by transnational cybercrime to national security. Discuss the role of international cooperation and India's institutional framework in addressing these threats.

EXAM YEAR	PAPER	SUBJECT
DAILY PRACTICE 21/11/2026	GS - III	Science & Technology

MARKS	WORD LIMIT
15	~250 words

Answer Hint

Cross-border cyberattacks, jurisdictional challenges, critical information infrastructure, ransomware, cyber espionage, Budapest Convention, UNTOC, CERT-In, NCIIPC, INTERPOL, public-private partnerships, cyber diplomacy.

Model Answer

Introduction

Cybercrime has evolved into a transnational security threat affecting financial systems, government networks, businesses and critical infrastructure. Digital connectivity allows perpetrators to operate across jurisdictions, complicating investigation and prosecution.

Major Challenges

1. **Jurisdictional limitations:** Cybercriminals can operate from foreign territories, creating difficulties in investigation, extradition and evidence collection.
2. **Critical infrastructure threats:** Attacks on banking, electricity, telecommunications and transport networks can disrupt essential services.
3. **Attribution difficulties:** Encryption, anonymisation and sophisticated attack techniques make identifying perpetrators challenging.

4. **Economic losses:** Ransomware, financial fraud and data breaches undermine business confidence and financial stability.
5. **State-linked threats:** Cyber espionage and attacks on strategic systems can have wider geopolitical and national security implications.

India's Institutional Framework

- **CERT-In:** Coordinates cybersecurity incident response under Section 70B of the IT Act, 2000.
- **NCIIPC:** Protects critical information infrastructure under Section 70A.
- **Indian Cyber Crime Coordination Centre (I4C):** Supports coordination among law enforcement agencies.
- **International cooperation:** India can strengthen information-sharing, mutual legal assistance and cooperation through INTERPOL and multilateral platforms.

Way Forward

India should strengthen cyber-forensics capacity, public-private partnerships, international evidence-sharing mechanisms, cyber awareness and resilience standards for critical infrastructure.

Conclusion

Cybersecurity requires coordinated national and international action. A resilient digital ecosystem, supported by effective institutions and cross-border cooperation, is essential for protecting national security and public trust.

BECOME IAS
AI POWERED UPSC PREP