Defence & Security · GS - III

Examine how state-sponsored cybercrime and cryptocurrency theft have emerged as challenges to international security. Suggest measures to strengthen global cybersecurity cooperation.

EXAM YEAR	PAPER	SUBJECT
DAILY PRACTICE 31/10/2026	GS - III	Defence & Security

MARKS	WORD LIMIT
10	~150 words

Answer Hint

State-sponsored cyberattacks; Lazarus Group; cryptocurrency theft; blockchain technology; sanctions evasion; critical infrastructure; cyber diplomacy; international cooperation

Model Answer

Introduction

State-sponsored cybercrime has emerged as a significant non-traditional security threat. Cyber operations attributed to North Korean groups, including the Lazarus Group, have reportedly targeted cryptocurrency exchanges and decentralised finance platforms.

Major Security Concerns

1. Illicit Financial Flows: Cryptocurrency theft can generate funds that may support prohibited activities and facilitate sanctions evasion.

2. Financial Vulnerability: Attacks on exchanges and DeFi platforms undermine investor confidence and expose weaknesses in digital financial infrastructure.

3. Attribution Challenges: Anonymity, cross-border networks and sophisticated techniques make identifying perpetrators and enforcing accountability difficult.

4. Geopolitical Risks: State-linked cyber operations can intensify international tensions and threaten critical digital infrastructure.

Way Forward

- Strengthen international information-sharing and joint cyber investigations.
- Improve cybersecurity audits, encryption and multi-factor authentication.
- Develop effective regulation of virtual digital asset service providers.
- Strengthen blockchain analytics and anti-money laundering mechanisms.
- Promote capacity-building and cooperation through international institutions.

Conclusion

Cybersecurity requires coordinated national capabilities and international cooperation to protect digital finance, critical infrastructure and global stability.

BECOME IAS
AI POWERED UPSC PREP