Defence & Security · GS - III

Critical law-enforcement databases are increasingly vulnerable to cyber intrusions. Discuss the implications of such breaches for national security, criminal justice and public trust. Suggest measures to strengthen their cybersecurity.

EXAM YEAR	PAPER	SUBJECT
DAILY PRACTICE 21/11/2026	GS - III	Defence & Security

MARKS	WORD LIMIT
15	~250 words

Answer Hint

Critical information infrastructure, sensitive law-enforcement data, identity theft, operational security, CERT-In, NCIIPC, zero-trust architecture, encryption, cyber resilience, international cooperation.

Model Answer

Introduction

Law-enforcement databases containing criminal records, warrants, biometric information and investigative details are essential to internal security. Their compromise can threaten policing operations and public safety.

Major Implications of Cyber Intrusions

1. **National security:** Exposure of sensitive intelligence and investigative information can compromise ongoing operations.
2. **Criminal exploitation:** Stolen records may facilitate identity theft, impersonation, extortion and targeted attacks against law-enforcement personnel.
3. **Criminal justice:** Manipulation of warrants or criminal records can lead to wrongful detention, investigative errors and disruption of judicial processes.

4. **Institutional credibility:** Repeated breaches weaken public confidence in government institutions and digital governance.

Measures to Strengthen Cybersecurity

- **Zero-trust architecture:** Continuously verify users, devices and access requests rather than relying solely on network boundaries.
- **Encryption:** Protect sensitive information during storage and transmission.
- **Access control:** Apply role-based permissions, multi-factor authentication and periodic access audits.
- **Continuous monitoring:** Strengthen threat detection, vulnerability assessments and incident-response mechanisms.
- **Institutional coordination:** Improve cooperation among CERT-In, NCIIPC, law-enforcement agencies and intelligence organisations.
- **Resilience:** Maintain secure backups, disaster-recovery systems and regular cybersecurity exercises.

Conclusion

Digital policing must be supported by equally robust digital security. Protecting law-enforcement databases is essential not only for national security but also for the integrity of criminal justice and citizens' trust in public institutions.

BECOME IAS
AI POWERED UPSC PREP