Q10

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

UPSC Civil Services Mains 2021 · GS III · 10 marks · Cyber Security and Money Laundering

Challenges to internal security through communication networks, role of media and social networking sites in internal security challenges, basics of cyber security; money-laundering and its prevention.

## Core demand of the question

- Keeping in view India's internal security, analyse the impact of cross-border cyber attacks. Also discuss defensive measures against these sophisticated attacks
- Keep the explanation within a 10-mark length

## Revision summary

Cross-border cyber operations can stall critical infrastructure, rob finance, and steal state data without a kinetic raid.

Attribution problems let states and proxies hide behind criminal malware.

CERT-In, NCIIPC, Defence Cyber Agency, sector CERTs, and the IT Act are the Indian defensive core.

Segmentation, backups, vendor control, and phishing defence are the practical layer.

Resilience and international CERT cooperation matter more than a claim of perfect security.

## Introduction

Cross-border cyber attacks are a cheap way for a rival state, a proxy, or a criminal gang abroad to hit Indian banks, power, railways, and public trust without a visible soldier. For internal security they sit beside terrorism and subversion: the border is a router, not only a fence.

## Body

## Impact on internal security

- **Critical infrastructure** - power grids, ports, railways, oil, and telecom - can be slowed or blinded, which creates urban disorder without an explosion.
- **Banks, UPI rails, and markets** face theft, ransomware, and loss of confidence, which is a domestic stability problem as much as a cyber-crime problem.
- **Attribution is slow.** A server in a third country can mask a state or a non-state actor, which complicates response under international law.
- **Espionage and influence:** theft of defence and ministry data, and information operations that inflame communal or separatist fault lines.
- **Terror and insurgent use:** encrypted command, funding, and targeting of police databases. The 2020s pattern is mixed criminal-state toolkits (supply-chain malware, zero-days).

• Examples in the public domain include probes and incidents around **Kudankulam** (2019 reporting), **Mumbai power** disturbance debates in 2020, and repeated **Chinese and Pakistan-linked** campaign reporting by CERT-In and private firms. Exact operational detail is often classified; the strategic fact is persistent targeting.

## Defensive measures

• **CERT-In** as the national incident response node; **NCIIPC** for designated critical information infrastructure under the IT Act.

• **Network monitoring, segmentation, backups, and air-gapping** of the most sensitive control systems; no internet-facing SCADA by default.

• **Defence Cyber Agency** and service cyber commands for military networks; **NATGRID** and police cyber cells for the criminal layer.

• **IT Act** offences, data-protection rules as they evolve, **sector CERT** (finance, power), and mandatory incident reporting.

• **Supply-chain hygiene:** trusted telecom gear, software bills of materials, and audits of vendors.

• **International:** Budapest Convention cooperation even without full membership politics, bilateral CERT MoUs, and UN norms on not attacking critical civilian infra.

• **People:** phishing is still the main door. Training, zero-trust identity, and public-private drills matter more than a new logo.

## Limits

• **Perfect defence is false. The aim is** resilience**:** detect, isolate, restore, and attribute well enough to deter.

## Flow diagram

Cross-border actor -> Banks grid data

Banks grid data -> Internal security shock

CERT-In NCIIPC -> Detect isolate restore

Segmentation drills KYC of vendors -> Detect isolate restore

## Conclusion

Cross-border cyber attacks threaten Indian internal security by hitting money, power, data, and social trust from outside the fence. Defence is CERT-In, NCIIPC, segmented critical systems, cyber commands, and drills - resilience, not an unbreakable wall.

## Facts & figures

### CERT-In

Indian Computer Emergency Response Team: national cyber incident coordination.

### NCIIPC

National Critical Information Infrastructure Protection Centre under the IT Act, for designated CII.

### IT Act, 2000

Principal statute for cyber offences, interception architecture, and CERT-In directions.

### Defence Cyber Agency

Tri-service body to defend and operate in the military cyber domain.

### Kudankulam reporting, 2019

Public reporting of malware on a nuclear plant's administrative network; a warning on CII hygiene, with operational details partly disputed.