Q9

Discuss the potential threats of Cyber attack and the security framework to prevent it.

UPSC Civil Services Mains 2017 · 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

- Discuss potential threats from cyber attacks
- Discuss the security framework meant to prevent them, including law, CERT-In and critical-information infrastructure protection

Revision summary

Cyber attacks can halt power and payments, steal identity and defence data, and spread ransomware or disinformation.

The IT Act 2000 as amended in 2008 is the legal base for offences and CERT-In.

National Cyber Security Policy 2013 and NCIIPC address resilience and critical information infrastructure.

Sectoral CERTs, RBI rules, Cyber Swachhta Kendra and cyber police cells complete the map.

Skills, private compliance and a full data-protection law were still thin in 2017.

Introduction

India's banks, power grids, railways, Aadhaar-linked welfare and defence networks now run on **code**. A **cyber attack** can steal data, freeze payments, or damage industrial controls without a soldier crossing the border. Threats have grown with **Digital India**. The preventive framework is a mix of the **Information Technology Act**, **CERT-In**, sectoral teams, and the protection of **critical information infrastructure**. Capacity and private-sector hygiene still lag the threat.

Body

Potential threats of cyber attack

- **Critical infrastructure:** malware in power, telecom, ports, oil and nuclear plants can cause physical outage, as global incidents on industrial control systems have shown.
- **Financial crime:** phishing, ransomware, ATM and **SWIFT**-style fraud, and attacks on payment systems hit households and correspondent banking.
- **Data theft and espionage:** state and criminal actors target ministries, defence labs, and Aadhaar-seeded databases for identity and strategic intelligence.
- **Military and space networks:** degraded command, navigation or satellite links in a crisis would be a force multiplier for an adversary.

• **Disinformation and election systems:** compromise of parties, media or voter databases can undermine trust even without changing a result.

• **Supply-chain and insider** threats: tainted hardware, unpatched software, and contractors with excess privilege.

• **Distributed denial of service** on government portals during unrest or disaster blocks public communication.

• Attribution is hard, so **proxy and non-state** groups can strike with deniability.

Security framework to prevent it

• **Information Technology Act, 2000** (amended 2008): defines offences (including critical-infrastructure damage), electronic evidence, and intermediary duties; it is the basic criminal and compliance law.

• **Indian Computer Emergency Response Team (CERT-In)** under the IT Act: national incident response, advisories, vulnerability notes, and mandatory reporting directions for intermediaries and firms.

• **National Cyber Security Policy, 2013:** the Union's policy umbrella for a secure and resilient cyberspace, public-private partnership, and capacity building (a successor architecture has been debated, but 2013 remained the named policy).

• **National Critical Information Infrastructure Protection Centre (NCIIPC)** under the **National Technical Research Organisation**: identifies and advises protection of CII in power, banking, telecom, transport and government.

• Sectoral **CERTs** (finance, power, telecom) and **Reserve Bank** cyber guidelines for banks sit beside CERT-In.

• **National Cyber Coordination Centre** and related monitoring aim to share threat intelligence across agencies.

• **Cyber Swachhta Kendra** (botnet cleaning) and public digital-literacy drives try to cut the large pool of infected home machines.

• **Defence and intelligence** cyber units, and police cyber cells in States, handle military and criminal tracks; coordination among them is still a weak joint.

• Prevention also needs **procurement standards**, encryption, backup drills, and **Make in India** trusted electronics so the stack is not only a foreign black box.

• **Gaps:** shortage of skilled analysts, uneven private compliance, slow forensics, and the tension between **surveillance powers** and a still-thin data-protection statute in 2017.

Flow diagram

Threats CII finance espionage -> Incidents

IT Act 2000-2008 -> CERT-In response

NCIIPC -> Protect critical infrastructure

Policy 2013 sectoral CERTs -> Hygiene and drills

CERT-In response -> Hygiene and drills

Protect critical infrastructure -> Hygiene and drills

Conclusion

Cyber attacks threaten grids, banks, identity systems and military networks, often below the threshold of open war. India's framework is the IT Act, CERT-In, the 2013 policy, NCIIPC and sectoral rules. It will prevent damage only if reporting is honest, CII is actually hardened, and skills reach banks and State police, not only a few national teams.

Facts & figures

IT Act 2000

Principal law on cyber offences and electronic records; 2008 amendment strengthened provisions on critical infrastructure and CERT-In.

CERT-In

Indian Computer Emergency Response Team: national agency for cyber incident response, advisories and reporting directions.

NCIIPC

National Critical Information Infrastructure Protection Centre: NTRO body that guides protection of designated CII sectors.

National Cyber Security Policy 2013

Union policy for a secure cyberspace, PPP, and capacity building, still the named national policy framework in this period.

Cyber Swachhta Kendra

CERT-In botnet cleaning and malware detection service aimed at infected citizen and enterprise machines.