

6.Cert-In Role- Science & Technology

CERT-In- India's Frontline Defender against Cyber Threats.As India's internet user base crosses 100 crore, the Indian Computer Emergency Response Team (CERT-In) acts as the primary defense against rising cyber threats like AI-driven scams and ransomware. CERT-In works alongside specialized bodies like NCIIPC (critical infrastructure) and I4C (law enforcement) to protect the nation's \$20 billion cybersecurity industry.

The Rising Cyber Threat Landscape

Surge in Connectivity- With internet connections in India crossing the 100-crore mark in 2025, the digital attack surface has expanded significantly.

Evolving Threats- Frontline defenses are battling sophisticated threats such as ransomware, AI-driven scams, phishing, and organized financial fraud.

Economic Stakes- Protecting the Indian cybersecurity industry is critical, as it is valued at \$20 billion, comprises 400+ startups, and employs a workforce of 6.5 lakh professionals.

About Indian Computer Emergency Response Team (CERT-In)

- a) **Role-** India's frontline defense and national agency for cyber incident response.
- b) **Establishment-** Formed in 2004 under Section 70B of the Information Technology Act, 2000.
- c) **Nodal Ministry-** Operates under the Ministry of Electronics & Information Technology (MeitY).
- d) **Core Mandate-** Collection, analysis, and dissemination of information on cyber incidents.Forecast and alerts of cybersecurity incidents.Emergency measures for handling cybersecurity incidents.Coordination of cyber incident response activities.

Initiatives by CERT-In

1. Cyber Swachhta Kendra (CSK)

Function- Also known as the Botnet Cleaning and Malware Analysis Centre.

Service- Provides free tools to citizens and organizations to detect and remove malicious software (malware) and botnets from their devices.

2. National Cyber Coordination Centre (NCCC)

Function- Generates situational awareness of the cyberspace.

Mechanism- It **scans cyberspace metadata** (not content) to detect imminent threats and facilitates real-time information sharing among stakeholders.

3. Sectoral CSIRTs (Computer Security Incident Response Teams)

Network- CERT-In oversees a network of specialized response teams.

Sectoral Focus- Includes CSIRT-Fin (for the Financial Sector) and CSIRT-Power.

State-Level- Includes State-level CSIRTs to provide localized and specialized incident response.

4. Cyber Crisis Management Plan (CCMP)

Framework- A strategic framework mandated for all government bodies.

Objective- To counter major cyberattacks and ensure a coordinated recovery process to minimize downtime and damage.

5. Security Assurance Framework

Audits- A program where empanelled auditors conduct regular cybersecurity audits and vulnerability assessments.

Target- Focuses on government infrastructure and critical sector systems to ensure they meet security standards.

Other Institutional Frameworks Against Cyber Crimes

While CERT-In focuses on technical response, other bodies handle critical infrastructure, law enforcement, and coordination.

Institution	Function & Mandate	Parent Body / Act
NCIIPC (National Critical Infor- mation Infrastructure Protection Centre)	Critical Infrastructure Protection- Dedicated to protecting critical sectors like banking, telecom, power, transport, and strategic enterprises.	Section 70A of IT Act, 2000.

I4C (Indian Cybercrime Coordination Centre)	Law Enforcement Coordination- Coordinates police responses to cybercrime and manages the National Cyber Crime Reporting Portal.	Ministry of Home Affairs (MHA).
NCSC (National Cyber Security Coordinator)	Strategic Coordination- Ensures coordination among different agencies (military, intelligence, civilian) on national security matters.	National Security Council Secretariat (NSCS).

Citizen Financial Cyber Fraud Reporting and Management System (CFCFRMS)

Helpline- Features the national toll-free helpline '1930'.

Purpose- Enables immediate reporting of financial frauds to freeze the flow of stolen funds.

Source- <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2217537®=3&lang=1>