CERT-In [UPSC notes]

The Indian Computer Emergency Response Team (CERT-In) serves as the national agency for performing various functions in the area of cyber security in the country as per the provisions of section 70B of the Information Technology Act, 2000. In this article, you can read all about CERT-In and its significance for the IAS Exam.

CERT-In (The Indian Computer Emergency Response Team)

CERT-In has been operational since January 2004.

- CERT-In comes under the Ministry of Electronics and Information Technology (MeitY).
- It regularly issues advisories to organisations and users to enable them to protect their data/information and ICT (Information and Communications Technology) infrastructure.
- In order to coordinate response activities as well as emergency measures with respect to cyber security incidents, CERT-In calls for information from service providers, intermediaries, data centres and body corporates.
- It acts as a central point for reporting incidents and provides 24 × 7 security service.
- It continuously analyses cyber threats and handles cyber incidents tracked and reported to it. It increases the Indian Internet domain's security defences.
- CERT-In is leading the implementation of CCMP across Central Government Ministries/Departments/states and critical organisations operating in Indian cyberspace.
    - The Cyber Crisis Management Plan (CCMP) for Countering Cyber Attacks and Cyber Terrorism is a framework document for dealing with cyber-related incidents.

CERT-In Functions

In the IT Amendment Act 2008, CERT-In has been designated to perform the following functions in the area of cyber security -

- Collection, analysis and dissemination of information on cyber incidents.
- Forecast and alerts of cyber security incidents.
- Emergency measures for handling cyber security incidents.
- Coordination of cyber incident response activities.
- Issue guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents.
- Such other functions relating to cyber security as may be prescribed.

Cyber Attacks - Levels of concern

Threat Level	Condition
Level 1 Guarded Scope: Individual Organisation	Large scale attacks on the IT infrastructure of an organisation
Level 2 Elevated Scope: Multiple Organisations	Simultaneous large scale attacks onto IT infrastructure of multiple organisations
Level 3 Heightened Scope: State/Multiple States	Cyber attacks on infrastructure of critical sector and Government across a state or multiple states
Level 4 Serious Scope: Entire Nation	Cyber attacks on infrastructure of critical sector and Government across the nation.

CERT-In Issued Directions in April 2022

In April 2022, CERT-In issued directions relating to information security practices, procedures, prevention, response and reporting of cyber incidents for a safe and trusted internet.

- In order to facilitate incident response measures, CERT-In issued directions relating to information security practices, procedures, prevention, response and reporting of cyber incidents under the provisions of sub-section (6) of section 70B of the Information Technology Act, 2000.
- The directions cover aspects relating to -
    - synchronisation of ICT system clocks
    - mandatory reporting of cyber incidents to CERT-In (within six hours)
    - maintenance of logs of ICT systems (for 180 days)
    - subscriber/customer registrations details by Data centres, Virtual Private Server (VPS) providers, VPN Service providers, Cloud service providers
    - KYC norms and practices by virtual asset service providers, virtual asset exchange providers and custodian wallet providers.

These directions shall enhance the overall cyber security posture and ensure safe & trusted Internet in the country.