CERT-In: India's Frontline Defender against Cyber Threats

Mains: *GS-III – Science & Technology | Cyber Security Challenges*

Why in News?

As online fraud, phishing, ransomware, AI-driven scams, and threats to vital digital systems grow, the Government of India created CERT-In to fight cyber risks, anticipate future challenges, boost resilience, and keep India's digital progress secure, inclusive, and sustainable.

What about CERT-In?

- **Indian Computer Emergency Response Team (CERT-In)** – It is the national nodal agency responsible for ***responding to cybersecurity incidents in India.***
- **Established on** – January 19, 2004.
- **Operates under** – Ministry of Electronics and Information Technology (MeitY).
- **Legal mandate** – Section 70B of the Information Technology (IT) Act 2000.
- **Significance** – It provides the institutional depth for national cyber defence, protects India's rapidly expanding digital ecosystem and supports confidence in digital platforms and services.

How has India's digital ecosystem developed in recent years?

- **Expanding Digital Footprint** – Over the past decade, India's digital presence has grown rapidly due to internet access, smartphones, and public digital services.
- **Internet connections** – Reached 100.29 crore in 2025 (***crossed the milestone of 100 crore***), up from 25.15 crore in 2014.
- **Data usage** – Average monthly use per wireless subscriber rose 399 times—from 61.66 MB (2014) to 24.01 GB (2025), among the ***highest globally.***
- **Digital Payments Boom** – India's strong digital base has fueled rapid

growth in digital payments, with the *Unified Payments Interface (UPI)* emerging as the *backbone* of the country's payment ecosystem.

- In December 2025 alone, UPI processed over 21 billion transactions valued at more than Rs.27 lakh crore.
- **Government Response** – To address these risks, the Union Budget 2025–26 allocated Rs.782 crore for cybersecurity, underscoring the government's strong focus on securing India's digital infrastructure.

What are the core functions of CERT-In for the National Cybersecurity?

- **Promoting cybersecurity awareness** among organisations and citizens,
- **Facilitating information sharing** through its automated cyber threat exchange platform,
- **Sharing near-real time information** on existing and potential cyber threats across all sectors,
- **Collaborates internationally** with partners, industry, and academia, and coordinate for mitigation measures,
- Conducts regular training programmes, drills, and exercises.
- **Operating CSKs** for cyber hygiene and a Command & Control Centre for monitoring threats.
- **Institutionalising** responsible vulnerability disclosure
- **Supporting** incident investigations and assists law enforcement with cyber forensics.
- Guides organisations in implementing Cyber Crisis Management Plans (CCMP) to boost national preparedness.

What are the key achievements of CERT-In in 2025?

- **National Cyber Incident Response & Threat Intelligence –** In 2025, it handled over 29.44 lakh cyber incidents, issued 1,530 alerts, 390 vulnerability notes, and 65 advisories, and published 29 Common Vulnerabilities and Exposures (CVEs),
- **Cybersecurity Audits** – Empaneled 231 certified security audit organisations, with most audits focused on banking, finance, power, energy, and transport sectors to strengthen cybersecurity across government, public, and private ICT systems.
- **Capacity Building** – Organised 32 technical training programmes and 95 awareness sessions, trained 20,799 officers and cybersecurity professionals from government, PSUs, and industry.
- **Cybersecurity Drills & Preparedness** – Organised 122 cybersecurity drills/exercises (including tabletop).

- Participation from 1,570 organisations across defence, paramilitary, space, atomic energy, telecom, finance, power, oil & gas, transport, IT/ITeS, and state data centres.
- **Awareness Initiatives** – CERT-In conducted 95 awareness sessions covering 91,065 participants (including *National Cybersecurity Awareness Month (NCSAM) October 2025*).
- **Reports & Guidelines (2025)** – Includes Smart City Cybersecurity Guidelines, India Ransomware Report, Digital Threat Report 2024 for BFSI, Cyber Smart Kids Guide & Senior Citizens Best Practices, etc.

What are the key institutional structures supported by CERT-In?

- **Cyber Swachhta Kendra (CSK)** – The CSK Botnet Cleaning and Malware Analysis Centre is established to enhance cyber hygiene among citizens.
- It tracks network of infected devices (computers, mobiles, IoT, routers) and provides free tools and guidance for malware removal, works with industry, academia, and ISPs to alert users.
- **Coverage** (Dec 2025) - 98% of India's digital population, engaging 1,427 organisations onboarded; 89.55 lakh tool downloads.
- **Security Assurance Framework –** To strengthen the security of government and critical sector systems.
- Under this framework certified IT security audit organisations conduct regular audits, vulnerability assessments and penetration testing are undertaken.
- **National Cyber Coordination Centre (NCCC)** – It was implemented to monitors cyberspace at metadata level to detect potential cybersecurity threats for situational awareness.
- It facilitates real-time information sharing and supports timely preventive and response actions with States and organisations.
- **Computer Security Incident Response Teams (CSIRTs)** – CERT-In oversees a network of CSIRTs operating at the sectoral and State/UT levels. Sectoral CSIRTs support domains such as finance, power, and telecom, while State CSIRTs operate under respective State and UT governments.
- **Cyber Crisis Management Plan (CCMP)** – It provides structured guidance during major cyberattacks and cyber-terrorism incidents, to supports rapid response, recovery, and continuity of essential services, particularly for critical infrastructure.
- **CSIRT-Fin (Financial Sector) –** It is the dedicated Computer Security Incident Response Team for the *Banking, Financial Services, and Insurance (BFSI) sector,* which strengthens cybersecurity through

coordinated incident response, information sharing, and sector-specific guidance/support.
- **CSIRT-Power (Power Sector) –** It functions as an extended arm of CERT-In for the Power Sector, focuses on incident analysis, threat intelligence, audits, and vulnerability mitigation and works with CSK to address malware infections and enhance resilience.

How about the global recognition of India's cybersecurity leadership?

- **Growing International Standing** – India's cybersecurity efforts resonate globally due to CERT-In's scale, tech-driven approaches, and collaborative governance have positioned India as a credible and responsible stakeholder in the international cybersecurity ecosystem.
- **Global Cybersecurity Outlook, 2025** – Published by the World Economic Forum (WEF), highlighted CERT-In's AI-driven situational awareness systems for detecting malicious domains and phishing, and its real-time global threat intelligence sharing.
- **Cyber Resilience Compass Paper, 2025** – Published jointly by the WEF and the University of Oxford, CERT-In contributed to identifying seven critical domains of cyber resilience.
- **Joint AI Risk Report, 2025** – It was co-signed with France's ANSSI and other partners, advocated a risk-based approach for trusted AI systems, secure AI value chains, and address emerging AI-related cyber risks.

What lies ahead?

- Amid rising and complex cyber threats, CERT-In anchors India's cybersecurity ecosystem by identifying and mitigating risks, it has strengthened national cyber resilience.
- Its initiatives include institutional frameworks, sectoral & state CSIRTs to citizen centric awareness programmes to promote safe digital practices.
- International recognition of its AI-driven innovations highlights India's growing global leadership in cybersecurity.
- Collectively, these efforts reaffirm the Government of India's commitment to a safe, trusted, and secure digital future.

Reference

PIB | CERT-In: India's Frontline Defender against Cyber Threats

SHANKAR
IAS PARLIAMENT
Information is Empowering