Government Strengthens Cyber Resilience Against AI-Enabled Cyber Threats through AI-Driven Detection, Vulnerability Assessment and Threat Intelligence

CERT-In Conducts 10 Cyber Security Exercises on AI-Driven Cyber Threats with 1,470 Participants from 345 Government and Private Organisations

प्रविष्टि तिथि: 30 JUL 2026 2:55PM by PIB Delhi

The Government is cognizant of the evolving cyber security threats and challenges, including those arising from Artificial Intelligence (AI) enabled cyber threats. AI technologies may increase systemic cyber risks by enabling automated reconnaissance, rapid vulnerability exploitation, credential compromise and highly convincing multilingual social engineering campaigns. These capabilities lower attack costs, accelerate weaponization, and make phishing and impersonation attacks more scalable and difficult to detect.

The Government is committed to ensuring an open, safe, trusted and accountable cyberspace. Several legal, technical and administrative policy measures have been implemented to address the risks posed by AI-enabled cyber threats, enhance cyber resilience, and strengthen incident response capabilities, which inter alia include:

1. AI-driven situational awareness systems are deployed by the Indian Computer Emergency Response Team (CERT-In) to detect malicious domains and phishing activities for necessary mitigation.

2. CERT-In has extended AI-enabled vulnerability assessment for public-facing digital assets in a sandbox environment to detect and mitigate vulnerabilities.

3. CERT-In operates an automated cyber threat intelligence exchange platform for sharing tailored alerts with organisations across sectors for proactive threat mitigation actions.

4. CERT-In has conducted 10 tailored cyber security exercises and drills on the theme "Building Resilience against Frontier AI-driven Cyber Threats" during June–July 2026. These exercises involved 1,470 participants from 345 Government and private organisations across sectors such as Power, Telecom, Banking, Financial Services and Insurance (BFSI), Transport, Education, Health and Space.

5. The Certified Security Professional in Artificial Intelligence (CSPAI) program was launched by CERT-In and SISA in September 2024. This American National Standards Institute (ANSI) National Accreditation Board (ANAB) approved program aims to equip cybersecurity professionals with the skills to secure AI systems, proactively address AI-related threats, and ensure trustworthy AI deployment in business environments.

6. CERT-In conducts cyber security training programs in collaboration with Industry partners to upskill the cyber security workforce in Government, public and private sectors.

7. CERT-In is one of the international partners to co-sign the joint high-level risk analysis report on Artificial Intelligence (AI) entitled "Building trust in AI through a cyber-risk-based approach," published by the National Cybersecurity Agency for France (ANSSI) in February 2025.

8. Advisories and Guidelines:

i. CERT-In issues alerts and advisories regarding the latest cyber threats, vulnerabilities, and countermeasures to protect computers, networks, and data on an ongoing basis.
ii. CERT-In has issued guidelines in June 2026 requiring all Original Equipment Manufacturers (OEMs) and technology providers to implement AI-accelerated vulnerability protection, requiring AI-assisted security testing, continuous monitoring, patch management, and incident response frameworks to defend against AI-driven cyber threats.
iii. CERT-In has issued a "Blueprint for Reducing Exposure and Defending against AI-Assisted Vulnerabilities Exploitation in Digital Infrastructure" in May 2026, aimed at protecting digital infrastructure against rapidly evolving AI-driven cyber threats.
iv. CERT-In has issued an advisory titled "Defending Against Frontier AI Driven Cyber Risks" in April 2026, which outlined comprehensive measures for organizations, MSMEs, and individuals to strengthen protection against advanced AI-enabled threats.
v. CERT-In has issued technical guidelines in July 2025 for Bill of Materials (BOM) for software, hardware, Artificial Intelligence, Quantum Computing & Cryptography requirements to enhance the security and transparency of supply chains.
vi. CERT-In has issued an advisory in March 2025 depicting best practices for effective and responsible use of Generative AI solutions.
vii. CERT-In has published "Cyber Security Guidelines for Smart City Infrastructure" in February 2025 including measures for secure usage of Artificial Intelligence (AI) and Machine Learning (ML) for smart city infrastructure and applications.
viii. CERT-In has issued an advisory in November 2024 on deepfake threats and measures that need to be followed to stay protected against deepfakes.
ix. CERT-In has published a whitepaper in collaboration with Mastercard in August 2023, highlighting the increasing attacks on Application Programming Interface (API) and use of AI in mitigating these attacks.
x. CERT-In has issued an advisory in May 2023 on safety measures to be taken to minimize the adversarial threats arising from Artificial Intelligence (AI) based applications.

This information was submitted by Union Minister of State Shri Jitin Prasada in Lok Sabha on 29.07.2026.

****

Vinod Kumar / Kanishk Sharma

(रिलीज़ आईडी: 2291652) आगंतुक पटल : 1174