GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO. 717
TO BE ANSWERED ON: 05.12.2025

AI DRIVEN CYBERATTACKS

717. SHRI RITABRATA BANERJEE:

Will the Minister of ELECTRONICS AND INFORMATION TECHNOLOGY be pleased to state:

(a) the number of AI powered cyber attacks faced by Indian firms in the last three years, the year-wise details thereof;
(b) the number of AI powered cyber attacks faced by Government websites in the last three years the year-wise details thereof;
(c) whether any audit has been conducted by Government regarding the resilience of firms against AI powered cyber attacks, the details thereof; and
(d) the steps taken by Government to ensure that firms are equipped to deal with such cyber attacks, especially in the critical sectors, the details thereof?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI JITIN PRASADA)

(a) to (d): The Indian Computer Emergency Response Team (CERT-In) is designated as the national agency for responding to cyber security incidents under the provisions of section 70B of the Information Technology (IT) Act, 2000. As per the information reported to and tracked by CERT-In, the total number of cyber security incidents related to Indian entities observed during the last three years are given below:

Table: Number of cyber security incidents in Private sector organisations

Year	**Number**
2022	11,99,018
2023	13,88,073
2024	7,31,988

The Government has undertaken various initiatives to deal with cyber-attacks including those for critical sectors, which inter alia, include:

i. “The Safe & Trusted‟ pillar within the IndiaAI Mission aims to encourage the adoption of AI in a responsible manner with the principles of safety, security, transparency, and privacy embedded in the design of AI technology to mitigate the AI risks, placing the idea of “AI for All” at its very core.

ii. CERT-In has empanelled 231 security auditing organizations to support and audit implementation of Information Security Best Practices.

iii. CERT-In and National Critical Information Infrastructure Protection Centre (NCIIPC) carry out cybersecurity audits under Information Technology Act, 2000 and Rules made thereunder.

iv. NCIIPC undertakes vulnerabilities and risk assessment of Critical Information Infrastructure/ Protected Systems periodically and gives feedback to all concerned.

v. National Cyber Coordination Centre (NCCC), implemented by CERT-In, examines the cyberspace to detect cyber security threats. It shares the information with concerned organizations, state governments and stakeholder agencies for taking action.

vi. Cyber security mock drills are conducted regularly to enable assessment of cyber security posture and preparedness of various organisations.

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

viii. Cyber Swachhta Kendra (CSK) is a citizen-centric service provided by CERT-In, which extends the vision of Swachh Bharat to the Cyber Space. Cyber Swachhta Kendra is the Botnet Cleaning and Malware Analysis Centre and helps to detect malicious programs and provides free tools to remove the same. It also provides cyber security tips and best practices for citizens and organisations.

ix. CERT-In issues alerts and advisories regarding latest cyber threats/vulnerabilities and countermeasures to protect computers, mobile phones, networks and data on an ongoing basis.

x. CERT-In conducts regular cyber security trainings for IT/ cyber security professionals of Government, public and private sector organizations.

******