# O.I.H

GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO. 1503
TO BE ANSWERED ON: 01.08.2025

MEASURES TO PREVENT CYBER ATTACKS

# 1503. DR. BHIM SINGH:

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

(a) whether it is a fact that sophisticated techniques such as Artificial Intelligence (AI), deepfakes, social engineering and supply chain vulnerabilities are now being used in cyber attacks, thereby endangering not only citizens but also financial and technological institutions; and
(b) if so, the strategic, technical and monitoring measures taken by Government to prevent such threats and the effectiveness of these measures?

ANSWER

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

(a)and (b): Government remains cognizant and aware of sophistication and scale of cyber threats. “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.

Further, the Government has undertaken following initiatives to prevent cyber threats, which inter-alia includes:

i) The Indian Computer Emergency Response Team (CERT-In) is designed as the national agency for responding to cyber security incidents under the provisions of section 70B of the Information Technology Act, 2000.

ii) CERT-In works with other agencies involved in ensuring cybersecurity including Telecom Security Operations Centre (TSOC), India Cyber Crime Coordination Centre (I4C), National Centre Information Infrastructure Protection Centre (NCIIPC), etc.

iii) National Cyber Coordination Centre (NCCC) being 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.

iv) CERT-In issues alerts and advisories regarding latest cyber threats/vulnerabilities including malicious attacks using Artificial Intelligence and countermeasures to protect computers, networks and data on an ongoing basis. In this context, an advisory on safety measures to be taken to minimize the adversarial threats arising from Artificial Intelligence (AI) based applications was published in May 2023. Further, an advisory depicting best practices for effective and responsible use of Generative AI solutions was published in March 2025. CERT-In has also published an advisory in November 2024 on deepfake threats and measures that need to be followed to stay protected against deepfakes.

v) CERT-In has issued updated technical guidelines in July 2025 for Bill of Materials (BOM) for software, hardware, Artificial Intelligence, Quantum Computing & Cryptography requirements. These guidelines are aimed to enhance the security and transparency of supply chains for software, hardware & emerging technologies.

vi) CERT-In conducts joint cyber security training programs in collaboration with Industry partners to upskill the cyber security workforce in Government, public and private organizations with the latest skills. Technical training sessions in the area of AI-powered cybersecurity threats were conducted with experts from Industry to help the participants understand the latest threat landscape and best practices.

vii) The Certified Security Professional in Artificial Intelligence (CSPAI) program was launched by CERT-In in September 2024. The program aims to address the growing need for Secure and Responsible AI integration into business applications and processes. The CSPAI program equips cybersecurity professionals with the skills to secure AI systems, proactively address AI-related threats, and ensure trustworthy AI deployment in business environments.

viii) 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 in February 2025. The report advocates for a risk-based approach to support trusted AI systems and secure AI value chains.

ix) CERT-In 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.

x) To address supply chain concerns, the National Security Directive for Telecom Sector (NSDTS) has been implemented vide which only Trusted Products from Trusted Sources are inducted into Telecom Networks.

xi) Cyber security mock drills are conducted regularly to enable assessment of cyber security posture and preparedness of organizations in Government and critical sectors.

******