GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 1412
TO BE ANSWERED ON: 28.07.2021

CYBER ATTACK ON CRITICAL INFRASTRUCTURE

1412. SHRI PARVESH SAHIB SINGH VERMA:

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

(a) whether there have been attempts of cyber attacks on critical infrastructure of the country and if so, the details thereof and the reaction of the Government thereto;

(b) the steps taken by the Government to strengthen cyber security infrastructure of the country in recent years; and

(c) whether the country has the capability to launch offensive cyber operations to thwart enemy attacks and if so, the details thereof and the progress made by the country in this regard during the last five years?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI RAJEEV CHANDRASEKHAR)

(a): The Indian Computer Emergency Response Team (CERT-In) is serving as national agency for responding to cyber security incidents as per provisions of Section 70B of Information Technology Act, 2000. CERT-In receives inputs from its situational awareness systems and threat intelligence sources about cyber-attacks and malware infections in networks of entities across sectors and issues alerts to concerned organisations and Sectoral Computer Security Incident Response Teams (CSIRTs) for remedial measures.

(b) and (c): Government has taken following measures to strengthen cyber security posture and prevent cyber attacks:

i. 24x7 Security Monitoring Centre is in place at National Informatics Centre (NIC) for detecting and responding to security incidents related to NIC infrastructure and data centres. Additionally for enhancing Data Security, periodic security audits and vulnerability assessment of resources are performed followed by subsequent hardenings.
ii. 24X7 Cyber Security Incident Response mechanism is in place at Indian computer Emergency Response Team (CERT-In).

iii. CERT-In issues alerts and advisories regarding latest cyber threats/vulnerabilities and countermeasures to protect computers and networks on regular basis.

iv. CERT-In is sharing early warning threat intelligence alerts with over 700 organisations across sectors to enable active threat prevention.

v. Based on threat intelligence, appropriate counter measures are taken up by relevant agencies to mitigate such threats to ensure national security.

vi. Government has issued guidelines for Chief Information Security Officers (CISOs) regarding their key roles and responsibilities for securing applications / infrastructure and compliance.

vii. All the government websites and applications are to be audited with respect to cyber security prior to their hosting. The auditing of the websites and applications is conducted on a regular basis after hosting also.

viii. Government has empanelled security auditing organisations to support and audit implementation of Information Security Best Practices.

ix. Government has formulated Cyber Crisis Management Plan (CCMP) for countering cyber attacks for implementation by all Ministries/ Departments of Central Government, State Governments and their organizations and critical sectors.

x. Cyber security mock drills and exercises are conducted regularly to enable assessment of cyber security posture and preparedness of organisations in Government and critical sectors. 59 such drills have so far been conducted by CERT-In where 565 organisations from different States and sectors such as Finance, Defence, Power, Telecom, Transport, Energy, Space, IT/ITeS, etc participated.

xi. CERT-In conducts regular training programmes for network / system administrators and Chief Information Security Officers (CISOs) of Government and critical sector organisations regarding securing the IT infrastructure and mitigating cyber attacks.

xii. Government is operating the Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre). The centre is providing detection of malicious programs and free tools to remove the same.

xiii. Government has set up the National Cyber Coordination Centre (NCCC) to generate necessary situational awareness of existing and potential cyber security threats. Phase-I of NCCC is operational.

xiv. National Critical Information Infrastructure Protection Centre (NCIIPC) regularly issues Alert/ Advisory to strengthen the cyber security posture of the stakeholders.

****