GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO.3412
TO BE ANSWERED ON : 25.03.2021

CHINESE CYBER ATTACKS ON INDIAN INFRASTRUCTURE

3412. SHRI NARAIN DASS GUPTA:

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

(a) in light of recent reports on Chinese cyber-attacks on critical Indian infrastructure, whether Government can clarify the veracity of these reports; and
(b) if so, counter-measures taken by Government to deter further aggression?

ANSWER
MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI SANJAY DHOTRE)

(a) and (b): 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 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. It has been observed that attackers are compromising computer systems located in different parts of the world and use masquerading techniques and hidden servers to hide the identity of actual systems from which the attacks are being launched.

Alerts and advisories are issued to key organisations and sectoral CSIRTs for taking response and preventive measures against emerging cyber attacks.

Government has taken following measures to enhance the cyber security posture and prevent cyber attacks:

i. The Indian Computer Emergency Response Team (CERT-In) issues alerts and advisories regarding latest cyber threats/vulnerabilities and countermeasures to protect computers and networks on regular basis.
ii. Government has issued guidelines for Chief Information Security Officers (CISOs) regarding their key roles and responsibilities for securing applications / infrastructure and compliance.
iii. 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 will be conducted on a regular basis after hosting also.
iv. Government has empanelled security auditing organisations to support and audit implementation of Information Security Best Practices.
v. 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.
vi. Cyber security mock drills are being conducted regularly in Government and critical sectors.
vii. 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.

viii. 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.

ix. 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.

****