GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO. 3413
TO BE ANSWERED ON : 25.03.2021

PROTECTION TO PHARMA INDUSTRY AGAINST FOREIGN HACKERS

3413. SHRI SANJAY RAUT:

Will the Minister of ELECTRONICS AND INFORMATION TECHNOLOGY be pleased to state:
(a) whether it is a fact that a Chinese state-backed hacking group has in recent weeks targeted the IT systems of two Indian vaccine makers whose coronavirus shots are being used in the country's immunisation campaign;
(b) if so, the details thereof and Government's reaction thereto; and
(c) the details of steps taken or proposed to be taken by Government to protect pharma industry against foreign hackers?

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 and vulnerabilities in networks of entities across sectors and issued alerts to concerned organisations including in pharmaceutical sector 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.

(c): In tune with the dynamic nature of Information Technology and emerging cyber threats, continuous efforts are required to be made by owners and users to protect networks and data by way of hardening and deploying appropriate security controls. 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. Government has empanelled security auditing organisations to support and audit implementation of Information Security Best Practices.
iv. 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.
v. Cyber security mock drills are being conducted regularly in Government and critical sectors including Health sector.
vi. 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.

vii. 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.

viii. 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.

****