GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 4745
TO BE ANSWERED ON: 24.03.2021

CHINESE MALWARE ATTACK ON CRITICAL INFRASTRUCTURE

4745. SHRI MANISH TEWARI:
SHRI RAJMOHAN UNNITHAN:

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

(a) whether a Chinese state-sponsored group Red Echo has used malware techniques to gain a foothold in nearly a dozen critical nodes across the Indian power generation/transmission infrastructure, along with transmission substation and a coal-fired power plant and if so, the details thereof and the reaction of the Government thereto;

(b) whether the blackout in Mumbai on October 12, 2020 was a consequence of Chinese malware, Shadowpad and if so, the details thereof and the reaction of the Government thereto;

(c) whether India's Computer Emergency Response Team (CERT-In) received any evidence/findings about this from the cyber threat analysis group Recorded Future and if so, the details thereof;

(d) whether the Government has initiated any formal investigation into this cyber attack and if so, the details and the outcome thereof;

(e) whether the aforementioned malware has attacked any other critical infrastructure of the country and if so, the details thereof and the steps taken by the Government in this regard;

(f) the manner in which the Government plans to retaliate against such sophisticated cyber attacks; and

(g) whether the Government proposes to replace the existing Chinese made hardware in India's critical infrastructure in view of these cyber attacks and if so, the details thereof?

ANSWER

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

(a), (b) and (c): 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 issued alerts to concerned organisations and sectoral CERTs including in power 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.

(d), (e) and (f): Alerts and advisories are issued to key organisations and sectoral CERTs 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 is 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.

(g): There is no such proposal.

****