GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO. 245
TO BE ANSWERED ON: 21.07.2023

SETTING UP OF INFRASTRUCTURE TO ADDRESS CYBER ATTACKS

245 SHRI G.C. CHANDRASHEKHAR:

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

(a) the number of cyber attacks on country's critical infrastructure, year-wise, since 2018 till date;
(b) whether Government deems the current legal framework adequate to address the increase in the number of cyber attacks, especially in the light of recent security breaches;
(c) if not, whether Government is planning to introduce a new and targeted legislation to address above threat; and
(d) the measures taken by Government to set-up requisite infrastructure and schemes to provide for greater security against cyber attacks?

ANSWER

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

(a): The policies of the Government are aimed at ensuring an Open, Safe and Trusted and Accountable Internet for its users. With the innovation of technology and rise in usage of cyberspace and digital infrastructure for businesses and services, the cyber-attacks pose threat to confidentiality, integrity and availability of information and services. Government is fully cognizant and aware of various cybersecurity threats.

As per the Information Technology Act, 2000 ("IT Act"), Critical Information Infrastructure means computer resource whose incapacitation or destruction has debilitating impact on, *inter alia*, national security. The National Critical Information Infrastructure Protection Centre (NCIIPC) has been notified as the national nodal agency under the IT Act for Critical Information Infrastructure Protection. NCIIPC has informed that revealing details regarding cyber-attacks on such infrastructure would not be in the interest of the national security.

(b) and (c): Legal provisions exist in the Information Technology Act, 2000 to deal with cyber attacks. Sections 43 and 66 of the Act provides for penalty and punishment for cyber attacks. Section 70(3) of the Information Technology Act 2000 provides for penalty and punishment for unauthorized access of Critical Information Infrastructure/Protected Systems.

To help achieve the aim of Open, Safe and Trusted and Accountable Internet for digital nagriks, this Ministry engages with and receives inputs from the public and stakeholders, including in respect of changes required to existing legislation and the need to introduce fresh legislation. Once the legislative proposal is formulated, in accordance with the Government's policy on pre-legislative consultation, proposed legislation is published in the public domain and feedback/comments are invited from the public before introduction to relevant House of Parliament.

(d):The following measures have been taken by Government to set-up requisite infrastructure and schemes to provide for greater security against cyber-attacks:

(i) The National Cyber Security Coordinator under the National Security Council Secretariat coordinates with different agencies at the national level in respect of cybersecurity matters.

(ii) The Government has designated Indian Computer Emergency Response Team (CERT-In) as the national agency for responding to cyber security incidents. CERT-In operates an automated cyber threat exchange platform for proactively collecting, analysing and sharing tailored alerts with organisations across sectors for proactive threat mitigation actions by them.

(iii) The Government has established National Critical Information Infrastructure Protection Centre (NCIIPC) for protection of critical information infrastructure in the country. NCIIPC provides near real-time threat intelligence and situational awareness based on which regular alerts and advisories are sent to Critical Information Infrastructure (CII) / Protected System (PS) entities.

(iv) CERT-In has set up the National Cyber Coordination Centre (NCCC) to generate situational awareness regarding existing and potential cyber security threats.

(v) CERT-In operates the Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre). The centre provides detection of malicious programs and free tools to remove the same for citizens and organisations. The centre works in close coordination and collaboration with Internet service providers, academia and industry.

(vi) CERT-In has empanelled 150 security auditing organisations to support and audit implementation of Information Security Best Practices.

(vii) A Cyber Crisis Management Plan has been formulated by CERT-In for implementation by all Ministries and Departments of the Central / State Governments and their organisations and critical sectors help to counter cyber-attacks and cyber-terrorism.

(viii) Department of Telecommunications (DoT) has established Telecom Security Operations Centre (TSOC) for detection of threats and malicious traffic to facilitate protecting telecom infrastructure of the country.

(ix) Government websites and applications are audited with respect to cyber security and compliance with the Government of India Guidelines for Websites prior to their hosting. The auditing of the websites and applications is conducted on a regular basis after hosting also.

****