GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO. 2013
TO BE ANSWERED ON: 23.12.2022

CYBER ATTACKS ON CRITICAL INFRASTRUCTURE

2013 SHRI MALLIKARJUN KHARGE:

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

(a) the details of number of cyber attacks including major attacks on critical infrastructure systems that have taken place in the country in the last five years, year-wise;

(b) whether Government has any record of the origin of such cyber attacks, if so, the details thereof;

(c) whether Government is aware that many critical infrastructure systems are highly vulnerable to cyber attacks, which could pose a risk to the country's national security; and

(d) if so, the measures Government has taken to ensure that best practices with regard to cyber security are observed at such installations?

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 a borderless cyberspace, coupled with the anonymity, rapid growth of Internet, rise in cyber security incidents is a global phenomenon. 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):There have been attempts from time to time to launch cyber-attacks on the Indian cyberspace from systems outside the country. It has been observed that attackers are compromising computer systems located in different parts of the world and use sophisticated techniques/technologies and a network of proxy servers to mask the origin of the attackers.

(c) and (d): 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 cyber security threats including to critical infrastructure systems.

The following measures have been taken to ensure that best practices with regard to cyber security are observed at installations that have Critical Information Infrastructure:

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

(ii) The Central Government, through the Information Technology (Information Security Practices and Procedures for Protected System) Rules, 2018, has prescribed the practices and procedures for Critical Information Infrastructure notified by it as protected systems. These require the organisations having such protected systems to constitute an Information Security (IS) Steering Committee to approve the IS policies of the protected system and significant changes in its network configuration and applications, and to establish a mechanism for timely communication of cyber incidents. They also require the organisations to nominate a Chief Information Security Officer (CISO), establish an IS Management System, document the system's network architecture / authorised personnel / hardware and software inventory / IT security service level agreements, carry out vulnerability/threat/risk analysis, prepare a Cyber Crisis Management Plan, periodically carry out IS audits, establish cyber security and network operation centres, and take regular backup of logs. The CISO is required to maintain regular contact with the NCIIPC, is responsible for implementing security measures, and shares with and incorporates suggestions of NCIIPC in the IS related documents, plans etc. for the protected system.

(iii) The Indian Computer Emergency Response Team (CERT-In) is designated 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.

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

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

(vi) A Cyber Crisis Management Plan 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.

(vii) 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.

****