GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 1043
TO BE ANSWERED ON: 08.02.2023

CYBER ATTACK

1043   DR. ARVIND KUMAR SHARMA:
DR. BHARATIBEN DHIRUBHAI SHIYAL:

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

(a) whether it is a fact that India is one of the most cyber attack targetted countries in the world particularly from China and if so, the details thereof;
(b) whether the Government is making any efforts to tackle the said condition;
(c) if so, the details thereof; and
(d) if not, the reasons therefor?

ANSWER

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

(a): The Government is committed to ensure that the Internet in India is Open, Safe & Trusted and Accountable for all users. With the expansion of the Internet and more and more Indians coming online, the possibility that Digital Nagrik or citizens being exposed to user harms and criminality has also increased. Government is fully cognizant and aware of various cyber security threats.

Cyberspace being borderless, coupled with anonymity and wide scale reach of Internet, rise in cyber attacks and cyber security incidents is a global phenomenon. The Indian Computer Emergency Response Team (CERT-In) is mandated to track and monitor cyber security incidents in India. 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. According to analysis done by CERT-In, the Internet Protocol (IP) addresses of the computers from where the attacks appear to have originated are from a number of countries.

(b) to (d): A number of measures have been taken to enhance India's cyber security posture and to curb such incidents. These include the following:

(i.)   A Cyber Crisis Management Plan for countering cyber-attacks and cyber-terrorism, has been formulated by CERT-In, for implementation by all Ministries and Departments of the Central Government, State Governments and their organisations and critical sectors.
(ii.)   On observing an incident, CERT-In notifies the affected organisations along with remedial actions to be taken, and coordinates incident response measures with affected organisations, service providers, respective sector regulators and law enforcement agencies.
(iii.) Regular training programmes for network and system administrators and the Chief Information Security Officers of government and critical sector organisations are conducted by CERT-In, for securing the information technology infrastructure and mitigating cyber-attacks. A total of 42 training programmes were conducted, covering 11,486 participants, during the years 2021 and 2022.
(iv.)   CERT-In has been issuing alerts and advisories regarding latest cyber threats/vulnerabilities and countermeasures to protect computers and networks, on an ongoing basis.

(v.) Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre) is operated by CERT-In to detect malicious programs and free tools to remove the same, and to provide cyber security tips and best practices for citizens and organisations.

(vi.) 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.

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

(viii.) Cyber security mock drills are conducted to enable assessment of cyber security posture and preparedness of organisations in the government and critical sectors. 74 such drills have so far been conducted by CERT-In, in which 990 organisations from different States and sectors participated.

The National Cyber Coordination Centre has been set up to generate situational awareness regarding existing and potential cyber security threats.

CERT-In and the Reserve Bank of India (RBI) jointly carried out a cyber security awareness campaign on 'beware and be aware of financial frauds' through the Digital India Platform.

****