GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 1374
TO BE ANSWERED ON: 14.12.2022

CYBER ATTACKS

1374. SHRI MANISH TEWARI:

Will the Minister of ELECTRONICS AND INFORMATION TECHNOLOGY be pleased to state:
(a) whether it is a fact that cyber attacks have been increasing in the past five years in the Country;
(b) if so, the details thereof including the list wise number of such attacks between April 2017 to 30 November 2022;
(c) the number of cyber security incidents that have been carried out from outside the country between 01 April 2017 to 30 November 2022;
(d) whether there exists any cyber security policy for the country; and
(e) if so, the details thereof and if not, the reasons therefor including the progress made in creating such a policy?

ANSWER

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

(a) and (b):The policies of the Government are aimed at ensuring an Open, Safe and Trusted and Accountable Internet for its users. With the borderless cyberspace coupled with the anonymity, along with rapid growth of Internet, rise in cyber attacks and cyber security incidents is a global phenomenon. Government is fully cognizant and aware of various cyber security threats. The Indian Computer Emergency Response Team (CERT-In) is mandated to track and monitor cyber security incidents in India. In the recently notified cyber security direction CERT-In has now made it mandatory for all incidents to be mandatorily reported to CERT-In.

As per the information reported to and tracked by CERT-In, year-wise number of cyber security incidents areas below:

S. No.	Year	No. of Incidents
1	2017 (April to December)	41,378
2	2018	2,08,456
3	2019	3,94,499
4	2020	11,58,208
5	2021	14,02,809
6	2022 (till November)	12,67,564

(c): 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 the analysis by CERT-In, the Internet Protocol (IP) addresses of the computers from where the attacks appear to have originated from a number of countries.

(d) and (e): Government has published National Cyber Security Policy 2013 with the vision of building a secure and resilient cyberspace for citizens, businesses and Government, and the mission of protecting information and information infrastructure in cyberspace, building capabilities to prevent and respond to cyber threats, reducing vulnerabilities and minimising damage from cyber incidents, through a combination of institutional structures, people, processes, technology and cooperation.
Further, the Ministry of Home Affairs has issued National Information Security Policy and Guidelines to the Central Ministries as well as State Governments and Union territories with the aim of preventing information security breaches and cyber intrusions in the information and communication technology infrastructure.

******