GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION. NO. 3443
TO BE ANSWERED ON: 01.04.2022

DATA ON CYBER ATTACKS

3443. SHRI G.C. CHANDRASHEKHAR:
SHRI KUMAR KETKAR:
SMT. PHULO DEVI NETAM:`
DR. L. HANUMANTHAIAH:

Will the Minister of Electronics and Information Technology be pleased to state:

(a) whether Government records data regarding cyber attacks that have occurred against the Indian Government and Government-owned entities by foreign and domestic outfits;

(b) if so, the details thereof since 2016, by country of origin, and the average duration of time between detection and containment, if not, the reasons therefor; and

(c) whether Government has the capacity to handle a state of hybrid warfare?

ANSWER

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

(a) and (b): Government is fully cognizant and aware of various cyber security threats. Indian Computer Emergency Response Team (CERT-In) is mandated to track and monitor cyber security incidents in India.

CERT-In has reported that a total number of 5461, 33514, 70798, 85797, 54314 and 48285 cyber security incidents related to Government organisations during the year 2016, 2017, 2018, 2019, 2020 and 2021 respectively.

There are attempts from time to time to launch cyber attacks on Indian cyber space. It is observed that attackers compromise 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 launched.

According to the logs analyzed and made available to Indian Computer Emergency Response Team (CERT-In), the Internet Protocol (IP) addresses of the computers from where the attacks appear to be originated belong to various countries including Algeria, Brazil, China, France, Germany, Hong Kong, Indonesia, Netherlands, North Korea, Pakistan, Russia, Serbia, South Korea, Taiwan, Thailand, Tunisia, Turkey, USA, Vietnam etc.

CERT-In co-operates, works and coordinates incident response measures with international CERTs, overseas organizations and service providers as well as Law Enforcement Agencies.

(c): There is no such information available with this Ministry.

However, Government of India has taken measures to effectively address the cyber threats including hybrid threats which, inter alia, include:

(i) The Government has formulated a Cyber Crisis Management Plan (CCMP) to counter cyber-attacks and cyber terrorism for implementation by all Ministries/ Departments of Central Government, State/ UT Governments and their organizations, It also covers hybrid threats and influence via cyber channels. In addition, guideline documents and templates are published to assist development and implementation of sectoral Crisis Management Plans. The purpose of CCMP is to establish the strategic framework and guide actions to prepare for, respond to, and coordinate recovery from a cyber-crisis.

(ii) CERT-In regularly conducts workshops for Ministries, Departments, States & UTs and critical organizations to sensitize them about the cyber security threat landscape, which includes cyber vectors of hybrid influence. This enables them to prepare and implement the Cyber Crisis Management Plan. A total of 128 workshops have been conducted so far, out of these 31 CCMP workshops conducted during the year 2021

.

(iii) Cyber security mock drills and table top exercises are conducted regularly to enable assessment of cyber security posture and preparedness of organisations in Government and critical sectors which includes cyber vectors of hybrid influencing. 64 such drills are conducted by CERT-In where 820 organizations from different States and sectors participated.

****