GOVERNMENT OF INDIA
MINISTRY OF HOME AFFAIRS

LOK SABHA
UNSTARRED QUESTION NO. †2333

TO BE ANSWERED ON THE 02ND JANUARY, 2018/ PAUSHA 12, 1939 (SAKA)

THREAT OF CYBER ATTACK

†2333.   PROF. CHINTAMANI MALVIYA:
SHRI ALOK SANJAR:
DR. KRISHAN PRATAP:
DR. MANOJ RAJORIA:

Will the Minister of HOME AFFAIRS be pleased to state:

(a)   whether there are threats of cyber-attack from neighbouring countries;

(b)   if so, the details thereof and the reaction of the Government thereto;

(c)   whether the Government proposes to set up any mechanism to safeguard the details of single police investigation in its database;

(d)   if so, the details thereof along with the other measures taken to deal with cyber crimes and developing a holistic policy for meticulous enforcement of cyber laws in the country;

(e)   whether the Government proposes to sign any agreement with USA to control cyber crimes; and

(f)   if so, the details thereof?

ANSWER

MINISTER OF STATE IN THE MINISTRY OF HOME AFFAIRS
(SHRI HANSRAJ GANGARAM AHIR)

(a) & (b): There have been attempts from time to time to penetrate systems/devices of cyber networks operating in Government and its personnel. These attacks have been observed to be originating from the cyber space of a number of countries. The Government has taken various measures for enhancing the cyber security of information technology infrastructure in the country, these are:

i. Government has formulated Cyber Crisis Management Plan for countering cyber-attacks and cyber terrorism for implementation by all Ministries / Departments of Central Government, State Governments and their organizations and critical sectors.

ii. The Government has circulated Computer Security Policy and Guidelines to all the Ministries/Departments on taking steps to prevent, detect and mitigate cyber-attacks.

iii. The Indian Computer Emergency Response Team (CERT-In) issues alerts and advisories regarding latest cyber threats/vulnerabilities and countermeasures to protect computers on regular basis. Security tips have been published to enable users to secure their Desktops and mobile/smart phones. Tailored alerts are sent to key organisations to enable them to detect and prevent cyber-attacks.

iv. Cyber security mock drills are being conducted regularly to enable assessment of cyber security posture and preparedness of organizations in Government and critical sectors. Fifteen such drills have so far been conducted by CERT-In where 148 organisations from different States and sectors such as Finance, Defence, Power, Telecom, Transport, Energy, Space, IT/ITeS, etc. participated. In addition, three drills were conducted in

coordination with the Reserve Bank of India and the Institute for Development and Research in Banking Technology.

v. CERT-In conducts regular training programmes for network / system administrators and Chief Information Security Officers (CISOs) of Government and critical sector organisations regarding securing the IT infrastructure and mitigating cyber-attacks.

(c) & (d): For protection of information assets, Government of India has issued National Information Security Policy and Guidelines to all Government Organisations including law enforcement agencies for implementation. The Ministry of Electronics & Information Technology has also issued guidelines for appointment of Chief Information Security Officers and other steps to be taken by the Government Organisations.

Police and public order are State subjects and prevention, detection, investigation and prosecution of all types of crime including cyber-crimes is primarily responsibility of States. However, the Government of India supplements the efforts of States by providing funding and training support for strengthening their law enforcement machineries.

(e) & (f): Framework for India-US Cyber Relationship was signed on 30.08.2016. It, inter-alia, provides for setting up sub-group on law enforcement cooperation along with designated Point of Contact by both sides to address cross-border cyber-crimes.

****