GOVERNMENT OF INDIA
COMMUNICATIONS AND INFORMATION TECHNOLOGY
LOK SABHA

UNSTARRED QUESTION NO:2426
ANSWERED ON:05.02.2014
CYBER ATTACKS AND TERRORISM
Mahtab Shri Bhartruhari;Venugopal Shri P.

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

(a) whether the Indian cyber space is becoming more vulnerable to cyber attacks and terrorism;

(b) if so, the details thereof and the number of incidents of cyber attacks particularly from hostile nations reported during the last three years and the current year;

(c) whether the Government proposes to create National cyber Coordination Centre, a multi-agency body, to check cyber attacks and terrorism;

(d) if so, the details thereof and whether there is shortage of cyber professionals/ experts in the country;and

(e) if so, the details thereof and the action taken by the Government in this regard?

Answer

MINISTER OF THE STATE IN THE MINISTRY OF COMMUNICATIONS AND INFORMATION TECHNOLOGY (SHRIMILINDDEORA)

(a) and (b) There have been continuous attempts to penetrate Indian cyber networks and systems from the cyber space of a number of countries. It has been observed that the attackers compromise computer systems located in different parts of the world and use masquerading techniques to hide the identity of actual systems from which the attacks are being launched. Cyber space is virtual, borderless and anonymous due to which it becomes difficult to actually trace the origin of a cyber attack.

During the years 2011, 2012 and 2013 a total no. of 37306, 23014 & 24216 Indian websites were defaced by various hacker groups spread across worldwide. In addition, a total no. of 13301, 22060 & 71780 security incidents including phishing, scanning, spam, malicious code, website intrusions etc. were reported to the Indian Computer Emergency Response Team

(CERT-In) during the year 2011, 2012 and 2013 respectively.

(c), (d) and (e) The Government has initiated action to set up Cyber Coordination Centre to coordinate with multiple agencies and stakeholders for preventing cyber attacks, reducing vulnerability to cyber attacks and minimizing damage & recovery time from such attacks when they occur.

With the growth in Information Technology infrastructure and related applications, the scale and sophistication of cyber security incidents are on the rise. To address the needs emerging from such incidents on a continuous basis, adequate cyber security professionals with necessary skills and training are required. The National Cyber Security Policy 2013 announced by the Government envisages creation of a workforce of 500000 professionals in Cyber Security in the next five years through capacity building, skill development and training. The strategy aims to incubate skills and competencies in an ongoing manner in a public private partnership model to cover formal education, non formal education and awareness creation amongst citizens.

Government has implemented Information Security Education Awareness (ISEA) programme to develop skilled cyber security professionals across the country through formal and non formal education as well as awareness creation on cyber security.