GOVERNMENT OF INDIA
COMMUNICATIONS AND INFORMATION TECHNOLOGY
LOK SABHA

UNSTARRED QUESTION NO:1557
ANSWERED ON:06.03.2013
MONITORING OF SOCIAL NETWORKING SITES
Annayyagari Shri Sai Prathap;Meghwal Shri Arjun Ram ;Natarajan Shri P.R.;Ramkishun Shri ;Thamaraiselvan Shri R.;Venugopal Shri P.

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

:

(a) whether the incidents of cyber crimes/attacks have gained strength through social networking sites such as Facebook, Orkut, Youtube. Twitter, etc;

(b) if so, the details thereof and steps taken/proposed to be taken by the Government to monitor the content on these sites and prevent cyber crimes;

(c) whether the Government is working on any action plan for making an international grid to check the cyber attacks;

(d) if so, the details thereof and the steps taken by the Government in this regard; and

(e) the details of steps taken/being taken by other countries for foiling cyber attacks?

Answer

MINISTER OF STATE FOR COMMUNICATIONS AND INFORMATION TECHNOLOGY (SHRI MILIND DEORA)

(a) and (b): It has been observed that social networking sites are being misused for malicious purposes and committing Cyber Attacks / Cyber Crimes. These websites are being used by malicious people to harvest personal information of targeted users or group of users. The attackers create fake or untraceable profiles for joining groups of benign users and harvest information. This information is being used to impersonate persons and conduct identity theft and phishing attacks through social engineering. The Social Networking Sites are also misused for spreading malware. The mutual trust of users is also used in enticing users to click on links to malicious URLs and opening files containing malware. Taking advantage of the technology advancements, malware such as Trojans are being delivered onto users` systems. Malware such as Koobface. Bancorkut, Scrapkut Orkut Worm, Backdoor-CEP which steal user`s information and use fraudulently were reported to be propagating through social networking sites.

Indian Computer Emergency Response Team (CERT-In) issues alerts on specific malware, whenever such malware is observed to be spreading through Social Networking Sites. In addition, steps have been taken to create awareness among public, particularly young people, on incidents of cyber crimes which take place through social media sites. However, there is no proposal at present to monitor the content of Social Media sites.

(c) and (d): Cyber security is borderless and transnational. Accordingly, strengthening international cooperation to effectively deal with cyber security issues, has been one of the main focus areas of the Government. In this regard, Government is making concerted efforts to determine the ways and means of expanding the international collaboration.

Besides this, Indian Computer Emergency Response Team (CERT-In) takes cooperative efforts with the counterpart CERT Organizations in other countries to share information in a timely manner for preventing cyber attacks as well as collaborating for providing swift response to the incidents.

(e): Generically, the steps/measures being adopted by other countries for prevention of cyber attack enabling legal framework, assessing cyber security threats, vulnerability management, early warning and response, compliance and assurance, technology research and development, information sharing and cooperation and education & awareness.