

GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO.1321
TO BE ANSWERED ON: 25.07.2018

INCREASE IN CYBER CRIME

1321. SHRI NISHIKANT DUBEY:
SHRI RAVINDRA KUMAR PANDEY:

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

- (a) whether cases of cyber crime are increasing every passing year;
- (b) if so, the details thereof, year-wise for the last three years;
- (c) whether the present IT laws are adequate to deal with the growing cyber crimes/attacks; and
- (d) if not, the measures to be taken by the Government to ensure safety and security of software programmes and cyber network in the country

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI S.S. AHLUWALIA)

(a) and (b): As per the data maintained by National Crime Records Bureau (NCRB), Ministry of Home Affairs, a total of 9622, 11592 and 12317 cyber crime cases were registered during the years 2014, 2015 and 2016 respectively. This includes cases registered under the Information Technology (IT) Act, 2000 and related sections of Indian Penal Code and Special & Local Laws involving computer as medium/ target. Data for year 2017 is still under compilation by NCRB.

(c) and (d): The Information Technology Act 2000 has provisions to deal with prevalent cyber crimes. Government has taken a number of legal, technical and administrative measures to prevent cyber crimes. These *inter alia*, include:

- (i) Government has established National Critical Information Infrastructure Protection Centre (NCIIPC) as per the provisions of Section 70A of the Information Technology (IT) Act, 2000 for protection of critical information infrastructure in the country.
- (ii) The Indian Computer Emergency Response Team (CERT-In) issues alerts and advisories regarding latest cyber threats and countermeasures on regular basis. CERT-In has published guidelines for securing IT infrastructure, which is available on its website (www.cert-in.org.in).
- (iii) Government has set up National Cyber Coordination Centre (NCCC) to generate necessary situational awareness of existing and potential cyber security threats and enable timely information sharing for proactive, preventive and protective actions by individual entities.
- (iv) Government has launched the Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre). The centre is providing detection of malicious programs and free tools to remove the same for banks as well as common users.

- (v) National Information Centre (NIC), which provides IT / E-Governance related services to Government departments, protects the cyber resources from possible compromises through a layered security approach in the form of practices, procedures and technologies that are put in place. NIC has deployed state-of-the-art security solutions including firewalls, intrusion prevention systems, anti-virus solution. Additionally, periodic security audits of resources are performed followed by subsequent hardenings. These are complemented by round-the –clock monitoring of security events and remedial measures are carried out for solving the problems subsequently.
- (vi) Government has established security and safety test labs under Standardisation Testing and Quality Certification (STQC) Directorate. Three major labs are functioning at Delhi, Kolkata and Bengaluru for security assessment of software (including computer programmes).
