GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
STARRED QUESTION NO. *117
TO BE ANSWERED ON: 23.11.2016

ANTI-NATIONAL/SOCIAL ELEMENTS ON SOCIAL MEDIA

***117 SHRI RAM KUMAR SHARMA:**
SHRI RADHESHYAM BISWAS:

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

(a) whether anti-national and anti-social elements are taking undue advantages with impunity in committing crimes using state of the art communication techniques like social media, mobile apps etc.;

(b) if so, the details thereof and measures taken to restrict their use so as to prevent crime and anti-national activities;

(c) whether the Information Technology Act, 2000 take care of cyber security, mobile crimes and misuse and abuse of the social media;

(a) whether the Government proposes to amend the Act in the light of newer developments and if so, the details thereof; and

(b) whether AP Shah Expert Group in their recommendations urged privacy safeguards to be made applicable to both Government and Private Sector entities and if so, the details thereof and the reaction of the Government thereto?

ANSWER

MINISTER FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI RAVI SHANKAR PRASAD)

(a) to (e): A Statement is laid on the Table of the House.

STATEMENT REFERED TO IN REPLY TO LOK SABHA STARRED QUESTION *117 FOR 23.11.2016 REGARDING ANTI-NATIONAL/SOCIAL ELEMENTS ON SOCIAL MEDIA

(a) and (b): With widespread proliferation of new technologies like social media and mobile apps, etc. there are some negative elements who are misusing these technologies for committing cyber crimes. Such behavior is facilitated by virtual and borderless nature of cyber space, where anyone can open an account in any name including fake name from any part of the world. Most social networking sites do not do background information check and have their servers abroad.

As per National Crime Records Bureau (NCRB), a total of 5693, 9622 and 11592 cyber crime cases were registered during the years 2013, 2014 and 2015 respectively.

Government has taken various steps in the form of legal framework, emergency response, awareness, training, and implementation of best practices to prevent occurrence of cyber breaches and cyber crime. These include:

i) The Information Technology (IT) Act, 2000 as amended in 2008 provides a legal framework to address the issues connected with cyber crime, cyber attacks and security breaches of information technology infrastructure.
ii) Cyber Crime Cells have been set up in all States and Union Territories for reporting and investigation of Cyber Crime cases.
iii) Government has set up cyber forensic training and investigation labs in the States of Kerala, Assam, Mizoram, Nagaland, Arunachal Pradesh, Tripura, Meghalaya, Manipur and Jammu & Kashmir for training of Law Enforcement and Judiciary in these States.
iv) A number of Cyber forensics tools for collection, analysis, presentation of the digital evidence have been developed indigenously and such tools are being used by Law Enforcement Agencies.
v) Indian Computer Emergency Response Team (CERT-In) and Centre for Development of Advanced Computing (CDAC) are involved in providing basic and advanced training to Law Enforcement Agencies, Forensic labs and judiciary on the procedures and methodology of collecting, analysing and presenting digital evidence.
vi) Reserve Bank of India (RBI) issues Circulars/advisories to all Commercial Banks on phishing attacks and preventive / detective measures to tackle phishing attacks. RBI also issues advisories relating to fictitious offers of funds transfer, remittance towards participation in lottery, money circulation schemes and other fictitious offers of cheap funds.
vii) 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 are available on its website (www.certin.org.in). In order to detect variety of threats and imminent cyber attacks from outside the country, periodic scanning of cyber space is carried out.
viii) Cyber security mock drills are being conducted regularly to enable assessment of cyber security posture and preparedness of organizations in Government and critical sectors.
ix) CERT-In, is setting up a Botnet Cleaning and Malware Analysis centre for detection of computer systems infected by malware and to notify, enable cleaning and securing systems of end users to prevent further malware infections.
x) Industry associations such as Data Security Council of India (DSCI), NASSCOM, Cyber Forensic Labs, set up in certain States, have taken up tasks of awareness creation and training programmes on Cyber Crime investigation. Academia like National Law School, Bangalore and NALSAR University of Law, Hyderabad are also engaged in conducting several awareness and training programmes on Cyber Laws and Cyber crimes for judicial officers.
xi) Ministry of Electronics & Information Technology(MeitY) is implementing 'Information Security Education and Awareness (ISEA)' project to train professionals / Government officials and create mass information security awareness among citizens. The project is implemented by 51 institutions across the country. So far, 11,110 persons have been trained/undergoing training in various formal/non-formal courses focusing on Cyber Security. 2,384 Government personnel have been trained in direct training programs. CDAC Hyderabad has conducted 377 Awareness workshops for various user groups covering 42,379 participants from 22 States/UT.
xii) Government has established National Critical Information Infrastructure Protection Centre (NCIIPC) as per the provisions of Section 70A of the Information Technology Act for protection of Critical Information Infrastructure in the country.
xiii) Government has formulated 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.
xiv) Government has initiated setting up of National Cyber Coordination Centre (NCCC), under CERT-In 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.
xv) Government has notified the Information Technology (Intermediary Guidelines) Rules 2011 under Section 79 of the Information Technology Act. These rules require that the Intermediaries, including national and international social networking sites and matrimonial sites, shall observe due diligence while discharging their duties and shall inform the users

of Computer resources not to host, display, upload, modify, publish, transmit, update or share any information that is harmful, objectionable, affect minors and unlawful in any way. The said rules also require the intermediaries to appoint Grievance Officers to address the grievances received from users and affected individuals / organizations as and when received by them.

(c) and (d): The IT Act, 2000 as amended in 2008 provides legal framework to address various types of prevalent cyber crimes including mobile related crimes and misuse of the social media. Presently, there is no proposal with the Government to amend the Information Technology Act 2000.

(e): A Group of Experts chaired by Justice A P Shah submitted a report in October 2012 to the then Planning Commission covering international privacy principles, national principles, and emerging issues. A copy of the report is available on the archived website of erstwhile Planning Commission at http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf. No decision to accept the recommendations of the Report has so far been taken.

****