GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO. 643
TO BE ANSWERED ON: 27.06.2019

MECHANISM FOR CYBER SAFETY AND CRIME ISSUES

643. SHRI SYED NASIR HUSSAIN:

Will the Minister of Electronics & Information Technology be pleased to state:-
(a) whether government is considering to set up an institutional mechanism dedicated to cyber safety and crime issues and if so, the details thereof and if not, the reasons therefor; and
(b) the efforts made by Government to train and develop specialized manpower in this regard?

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

(a): 'Police' and 'Public Order' are State subjects as per the Seventh Schedule to the Constitution of India and States/UTs are primarily responsible for prevention, detection, investigation and prosecution of crimes through their law enforcement machinery. The Law Enforcement Agencies take legal action as per provisions of law against the cyber crime offenders.

The Information Technology Act, 2000 has provisions to deal with cyber safety and prevalent cyber crimes. Government has taken a number of legal, technical and administrative measures to address cyber safety and cyber crimes. These inter alia, include:

(i) Government has established National Critical Information Infrastructure Protection Centre (NCIIPC) for protection of critical information infrastructure in the country, as per the provisions of section 70A of the Information Technology (IT) Act, 2000.
(ii) 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.
(iii) Government has issued guidelines for Chief Information Security Officers (CISOs) regarding their key roles and responsibilities for securing applications / infrastructure and compliance.
(iv) Government has empanelled 84 security auditing organisations to support and audit implementation of Information Security Best Practices.
(v) All organizations providing digital services have been mandated to report cyber security incidents to CERT-In expeditiously.
(vi) 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.
(vii) Cyber security mock drills and exercises are being conducted regularly to enable assessment of cyber security posture and preparedness of organizations in Government and critical sectors. 43 such exercises have so far been conducted by CERT-In where organisations from different sectors such as Finance, Defence, Power, Telecom, Transport, Energy, Space, IT/ITeS sectors participated.

(viii) 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.

(ix) Government has setup 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. Phase-I of NCCC has been made operational.

(x) Ministry of Home Affairs (MHA) is implementing 'Cyber Crime Prevention against Women and Children (CCPWC)' scheme from NIRBHAYA funds of the Ministry of Women & Child Development (M/o WCD). Under this scheme, funds are released to all States / Union Territories for setting up of Cyber Forensic Training Lab, hiring of consultant for training lab and capacity building (Cyber awareness and cyber investigation) of Police officers, judges & prosecutors. Training labs have already been set up in Himachal Pradesh, Madhya Pradesh, Uttarakhand, Arunachal Pradesh, Uttar Pradesh and Telengana. States/UTs have informed that more than 5,000 police personnel, prosecutors and judicial officers have been trained. Further, MHA is also implementing Indian cyber Crime Coordination Centre (14C)' Scheme at an estimated cost of Rs. 415.86 crore which aims at providing a platform to deal with all types of cybercrime in a coordinated and comprehensive manner.

(b): Ministry of Electronics and Information Technology (MeitY) has taken following initiatives for capacity building in cyber security:

(i) Under the Information Security Education and Awareness (ISEA) Project Phase-I (2005-2014), more than 44,000 candidates were trained in various formal/non-formal courses in Information Security through 40 institutions (including IISc. Bangalore, TIFR Mumbai, 4 IITs, 15 NITs, 4 IIITs, 7 Govt. Engineering Colleges and select centres of CDAC/NIELIT). Around 100 Government officials, covering NIC, ICERT, STQC, CDAC, NIELIT, ERNET, Scientists from MeitY, etc. were trained as Master Trainers in the area of Information Security. The ISEA Project Phase-II project aims to train more than 1 lakh candidates in various formal/non-formal courses & more than 13,000 Government officials by March 2020.

(ii) Further, 43,322 candidates have been trained/under-going training in various formal/non-formal courses through 52 institutions. Besides this, around 2.2 lakh candidates are under-going training / trained in affiliated colleges of 5 Technical Universities participating in the project. In addition, institutions have reported 710 paper publications in Cyber Security Domain.7,349 Government Officials have been trained in the area of Information Security through 12 centres of C-DAC/NIELIT and ERNET India. In addition, 1,016 Government officials trained through e-learning courses. Besides this, 836 general awareness workshops on Information Security have been organized across the country for various user groups covering 95,161participants.

(iii) MeitY, in collaboration with Data Security Council of India (DSCI), has set up Cyber Forensic Labs at Mumbai, Bengaluru, Pune and Kolkata for awareness creation and training programmes on cyber crime investigation. National Law School, Bangalore and NALSAR University of Law, Hyderabad are also engaged in conducting several awareness and training programmes on cyberlaws and cyber crimes for judicial officers. Mumbai, Pune, Bangalore and Kolkata and in north-eastern States at respective Police headquarters to train LEA officials (Police) in cyber crime detection. Using these facilities, more than 28000 Police /LEA personnel have been trained.

(iv) Further, cyber security is increasingly getting introduced in curriculum of schools and colleges every year. Many universities and institutions are offering PhD and Master degree specializing in Cyber Security/Information Security. Vocational training program

on cyber security have been introduced by Ministry of Skills Development and Entrepreneurship, as well as in universities like IGNOU.

(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. 24 trainings covering 845 participants were conducted in the year 2018.

****