GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS & INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO.1699
TO BE ANSWERED ON: 09.03.2018

PACT WITH COUNTRIES FOR EXCHANGE OF INFORMATION ON CYBER CRIMES

1699. SHRI R. VAITHILINGAM:

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

(a) whether it is a fact that India is currently working towards bilateral pact with around 15 countries for exchange of information on cyber crimes;
(b) if so, the details thereof
(c) whether it is also a fact that Government has taken several steps to check cyber crimes such as legal, policy and institutional; and
(d) if so, the details thereof

ANSWER

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

(a) and (b): No Sir. However, the Indian Computer Emergency Response Team (CERT-In) has entered into Memorandum of Understanding (MoU) with its overseas counterpart agencies/Computer Emergency Response Teams (CERTs) of United States of America (USA), United Kingdom, Japan, South Korea, Australia, Malaysia, Singapore, Canada, Vietnam, Uzbekistan and Bangladesh for information exchange and collaboration for cyber security incident response.

(c) and (d): Government has taken a number of legal, technical, policy and institutional measures to check incidents of cyber crimes. These *inter alia*, include:

(i) Enactment of the Information Technology (IT) Act, 2000 which has adequate provisions for dealing with prevalent cyber crimes.

(ii) 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. NCIIPC has been regularly advising the critical information infrastructure (CII) sector organisation to reduce vulnerabilities to all kinds of threats and attacks, by sharing threat intelligence, guidelines, best practices and frameworks for protection and guiding them with policies and protection strategies. In addition, training and awareness programs are regularly conducted to improve the cyber hygiene in CII organisations.

(iii) 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. Tailored alerts are sent to key organisations to enable them to detect and prevent cyber attacks.

(iv) Government has initiated setting up of National Cyber Coordination Centre (NCCC) in 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. Phase-I of NCCC has been made operational.

(v) 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.

(vi) The Ministry of Home Affairs has recently setup a Cyber & Information Security (CIS) Division to look into relevant matters relating to cyber-crime & information security. Ministry of Home Affairs is implementing a scheme 'Cyber Crime Prevention against Women and Children' (CCPWC) from NIRBHAYA funds during the period 2017-2020, under which Rs 82.8 crore as Grants-in-Aid have been disbursed to the States/UTs for setting up of one cyber forensic training laboratory in each State/UT and the scheme also aims to train 27,500 police personnel across the country in the field of cyber domain.

(vii) Ministry of Home Affairs has issued advisories to all the States/UTs for taking various steps for prevention of cybercrime, which are available on its website www.mha.gov.in.

(viii) Cyber Crime Cells have been set up in all States and Union Territories for reporting and investigation of cyber crime cases.

(ix) 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 personnel and Judiciary in these States.

(x) Cyber security mock drills are being conducted regularly to enable assessment of cyber security posture and preparedness of organizations in Government and critical sectors. 15 such drills have so far been conducted by CERT-In where 148 organisations from different States and sectors such as Finance, Defence, Power, Telecom, Transport, Energy, Space, IT/ITeS, etc participated. In addition 3 drills were conducted in coordination with The Reserve Bank of India and The Institute for Development and Research in Banking Technology.

(xi) A number of Cyber forensics tools for collection, analysis and presentation of the digital evidence have been developed indigenously and such tools are being used by law enforcement Agencies.

(xii) Government has formulated Cyber 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.

(xiii) 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. 22 training programs covering 610 participants were conducted during the year 2017.

*****