

- (iii) All the new government websites and applications are to be audited with respect to cyber security prior to their hosting. The auditing of the websites and applications is to be conducted on a regular basis after hosting.
- (iv) Government has empanelled 69 security auditing organisations to support and audit implementation of Information Security Best Practices.
- (v) Government has issued general guidelines for Chief Information Security Officers (CISOs) regarding their key roles and responsibilities for securing applications/infrastructure and compliance.
- (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 30 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 etc participated.
- (viii) 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.

Curbing fake news over internet and mobile platforms

2817. SHRI SANJAY SINGH: Will the Minister of ELECTRONICS AND INFORMATION TECHNOLOGY be pleased to state:

- (a) whether it is a fact that tens of citizens have been lynched due to hatred spread by fake & news over internet and mobile platforms, like WhatsApp;
- (b) if so, how does the Ministry plan to tackle the issue and spread digital literacy;
- (c) whether an amendment of IT Act or bringing a new policy is under consideration of the Government to overcome this problem; and

(d) how would Government control fake news if servers of companies are based outside the country?

THE MINISTER OF STATE IN THE MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY (SHRI S.S. AHLUWALIA): (a) There are media reports about increase in fake news, misinformation/disinformation on internet and mobile platforms particularly using WhatsApp platform leading to citizens being lynched. Ministry of Electronics and Information Technology (MeitY) took note of this and issued a notice to WhatsApp on 03.07.2018. In their response submitted on the same day, WhatsApp has conveyed a number of steps taken by them to address the issue of fake news propagated using their platform. In particular, they have shared the strategy of "Giving people the controls and information they need to stay safe" and "To work proactively to prevent misuse on WhatsApp". Subsequently on 19.07.2018, Government issued second notice to WhatsApp conveying that they need to come out with more effective solutions that can bring in accountability and facilitate enforcement of law in addition to the promised efforts towards labelling forwards and weeding out fake news.

(b) Government has taken several initiatives for user awareness relating to cyber safety including hatred spread by fake news over internet and mobile platforms including on WhatsApp. MeitY, through a program namely Information Security Education & Awareness (ISEA), has been highlighting the importance of following the ethics while using Internet and advice not to share rumours/fake news. Ministry of Home affairs (MHA) has also issued a number of advisories which includes advisory on untoward incidents in the name of protection of cows dated 09.08.2016, advisory on cyber crime prevention and control dated 13.01.2018 and also an advisory on incidents of lynching by mobs in some States fuelled by rumours of lifting/kidnapping of children dated 04.07.2018. Pursuant to the directions of the Supreme Court's order dated 17.07.2018 in WP(C) 754/2016, MHA has issued a directive on 23.7.2018 to all States for implementation of directions of the apex court and has constituted a Group of Ministers and a High level Committee to make recommendations in this matter.

Government has also asked WhatsApp to convey various steps taken by them to deal with fake.

(c) Government constantly works on strengthening legislative and enforcement mechanism, as and when need arises.

(d) Government is fully committed to freedom of speech and expression and privacy of its citizens as enshrined in the constitution of India. Government does not regulate content appearing on Internet. Law enforcement agencies take appropriate action on posting of malicious content on Internet on specific case-to-case basis.

The Information Technology (IT) Act, 2000 has provision for removal/disablement of malicious content appearing on Internet. Section 79 of the Act provides that intermediaries are required to follow due diligence. The Information Technology (Intermediary Guidelines) Rules, 2011 notified under this section prescribes that the intermediaries 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 or is unlawful in any way.

Further, section 69A of the IT Act empowers Government to block any information generated, transmitted, received, stored or hosted in any computer resource in the interest of - (i) sovereignty and integrity of India, (ii) defence of India, (iii) security of the State, (iv) friendly relations with foreign States, (v) public order, or (vi) for preventing incitement to the commission of any cognizable offence relating to above. Towards more effective enforcement, Ministry of Home Affairs (MHA) has been regularly interacting with popular social media sites like WhatsApp, Facebook, Twitter, YouTube etc.

E-KYC user agency licence

2818. SHRI VIVEK K. TANKHA: Will the Minister of ELECTRONICS AND INFORMATION TECHNOLOGY be pleased to state:

- (a) the number of companies which have been approached for availing e-KYC User Agency licence from private companies for providing services till date, both global and local respectively;
- (b) the deposit amount that has been received from these agencies; and
- (c) in which account/fund the same is being kept and how the said amount has been utilized by Government and under what authority?

THE MINISTER OF STATE IN THE MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY (SHRI S.S. AHLUWALIA): (a) Unique Identification Authority of India (UIDAI) offers Aadhaar authentication services to the entities