Challenges to internal security through communication networks, role of media and social networking sites in internal security challenges, basics of cyber security; money-laundering and its prevention

The Cambridge Analytica scandal, the Pegasus spyware attack on WhatsApp and the growing misuse of social media platforms to spread misinformation have made governments world over, including in India, realise the limitations of existing laws in dealing with the misuse of these platforms.

Prelims and Mains focus: about Pegasus spyware, the cyber threat, challenges and ways to address it

Need for stricter regulation of social media

- The need for greater regulation of social media companies stems from the growing feeling that they are not doing enough to curb the misuse of their platforms.
- In recent times, many of them have been involved in brushes with the government and courts. For instance, short-video app TikTok was accused of promoting pornography among teens and temporarily banned from app stores following a Madras high court order;
- WhatsApp was slammed for not being able to curb fake messages which led to several cases of mob lynchings in 2018 and, more recently, for the Pegasus spyware attack.
- Twitter too has been criticised for failing to curb hate speech.

What are the remedial proposals?

- While forcing companies to have a nodal officer in the country can make these platforms more accountable to legal requests, it also makes them vulnerable to government pressure.
- Having offices in India allows the government to exert extralegal pressure on the company officials by forcing them to comply with informal requests. It is only useful if the intermediaries are willing to push back on the pressure and not entertain any informal request from the government.
- China-based TikTok, in a statement, emphasised that it is committed to respecting local laws and actively coordinates with law enforcement agencies through an India-based grievance officer. TikTok claims to have removed six million videos between July 2018 and April 2019 for violation of its guidelines.
- Some of these proposals have been flagged on grounds of privacy. For instance, the traceability clause is going to have a huge impact on specific platforms such as WhatsApp and Telegram that encrypt all messages and calls. Enforcing traceability and deploying technology based automated tools to proactively identify and disable public access to malicious content will force them to break or lower the encryption as has been pointed out by industry in the past.
- WhatsApp maintained its official stance from February and reiterated that what is contemplated by the rules is not possible today given the end-to-end encryption that it
provides. The rules would require the company to re-architect WhatsApp, which would lead to a different product, one that would not be fundamentally private.

India position vis-a-vis USA

- The fact that India doesn’t have an encryption law per say also complicates the scenario. In fact, section 84A (introduced after an amendment in 2008) of IT Act 2000 has specific provisions authorizing central government for coming up with a policy on encryption. It has been 11 years but there is still no law on it.
- Further, to ensure that companies abide by the proposed rules and furnish information within 24 hours, the government will have to address hurdles in mutual legal assistance treaty between India and the US, which is why many of these requests take a lot of time to process. The target of the government should be having an executive agreement with the US under the Cloud Act.
- The US has significant stakes in the data localization debate as many of the companies are based in the US, and that can be used as leverage to negotiate such an agreement. That will allow law enforcement agencies in India to have expedited access to information held by platforms which are based outside the country.