Syllabus subtopic: Awareness in the fields of IT, Space, Computers, robotics, nanotechnology, bio-technology and issues relating to intellectual property rights.

News: Govt. questions WhatsApp after spyware is used for snooping

Prelims focus: about Pegasus spyware

Mains focus: Cyber technology and threats related to it

Background

WhatsApp has been used to spy on journalists and human rights activists in India earlier this year. The surveillance was carried out using a spyware tool called Pegasus, which has been developed by an Israeli firm, the NSO Group.

- The surveillance was carried out “between in and around April 2019 and May 2019” on users in 20 countries across four continents.
- In response, WhatsApp has sued the NSO Group in a federal court, accusing it of using WhatsApp servers in the United States and elsewhere “to send malware to approximately 1,400 mobile phones and devices (‘Target Devices’) for the purpose of conducting surveillance of specific WhatsApp users (‘Target Users’).”

Main Concern

- Tools that enable surveillance into our private lives are being abused, and the proliferation of this technology into the hands of irresponsible companies and governments puts us all at risk.
- WhatsApp, which is owned by Facebook, is the world’s most popular messaging app, with more than 1.5 billion users worldwide. About a quarter of those users — more than 400 million, or 40 crore — are in India, WhatsApp’s biggest market.

About Pegasus and its modus operandi

- It is a spyware that works by sending an exploit link, and if the target user clicks on the link, the malware or the code that allows the surveillance is installed on the user’s phone.
- Pegasus is installed without the user’s knowledge or permission.
- Once Pegasus is installed, the attacker has complete access to the target user’s phone.
- Pegasus delivers a chain of zero-day exploits to penetrate security features on the phone and installs Pegasus without the user’s knowledge or permission.
- A “zero-day exploit” is a completely unknown vulnerability, about which even the software manufacturer is not aware, and there is, thus, no patch or fix available for it.
Way ahead

- The government has pulled up WhatsApp for not disclosing to Indian authorities the details of the spyware attack launched on Indian citizens through the Israeli software Pegasus, despite at least a couple of high-level meetings between the two sides in the past few months.
- However, WhatsApp appeared to counter the Indian government, saying it had in May "quickly resolved a security issue and notified Indian and international government authorities."
- However, the government points out that though the WhatsApp informed CERT-In, or the Indian Computer Emergency Response Team, it failed to communicate the fact that Indian citizens had been affected by it.
- WhatsApp was legally bound under Section 70(B) of the IT Act, 2000 to inform the government about the details of such attacks (on Indian citizens), which they failed to.