6. Spyware Pegasus

Prelims: Science & Technology

Mains: GS-III Role of External state in creating Challenges to Internal Security

Why in News?

- The popular messaging platform WhatsApp was 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.
- WhatsApp sued the NSO Group in a federal court in US accusing it of using WhatsApp servers in the United States and elsewhere to send malware to approximately 1,400 mobile phones and devices.

Pegasus:

- All spyware do what the name suggests — they spy on people through their phones.
- Pegasus 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.
- A presumably newer version of the malware does not even require a target user to click a link.
- Once Pegasus is installed, the attacker has complete access to the target user's phone. The first reports on Pegasus's spyware operations emerged in 2016, when Ahmed Mansoor, a human rights activist in the UAE, was targeted with an SMS link on his iPhone 6.

Method of working:

- A Pegasus operator must convince a target to click on a specially crafted 'exploit link' which allows the operator to penetrate security features on the phone.
- This automatically installs Pegasus without the user's knowledge or permission.
- Once the phone is exploited and Pegasus installed, it begins contacting the operator's command and control and send back the target's private data, including passwords, contact lists, events, text messages, and live voice calls from popular mobile messaging apps.
- The operator can even turn on the phone's camera and microphone to capture activity in the phone's vicinity.