Pegasus Spyware

[UPSC Notes]

What is Pegasus Spyware

The Pegasus is spyware that was developed by an Israeli firm, the NSO Group in 2010.

- This spyware was first discovered in an iOS version in 2016 and it was a little different from the android version,
- The Pegasus spyware was able to read toe SMS, and emails, take screenshots, access contacts, and browser history, and listen to calls of the victims.
- Hackers can hijack the phone's camera and microphone as well, and turn it into a real-time surveillance device
- Pegasus is also able to send back the hacker the target's data, including passwords, contact lists, live voice calls, text messages, and calendar events from the popular mobile messaging apps.
- It is used as a tool to track terrorists and criminals for targeted spying.
- The NSO Group has stated that it sells this spyware only to the governments.

How Does Pegasus Work?

Pegasus spyware exploits undiscovered issues or bugs. Due to this, the phone can be infested even if it has an updated security system.

- In 2016 smartphones were infected with a technique called 'spear-fishing'. In this method, the emails of text containing a malicious link were sent to the target phone, and then it was activated when the target clicked the link,
- In 2019, Pegasus evolved and interaction was not required by the target. Pegasus was able to infiltrate a device with a missed call on WhatsApp, and delete the record as well which would make it impossible for the user to find out that he/she has been targeted.
- In the same year, WhatsApp said Pegasus exploited a bug in its code to infect more than 1400 iPhones and Android Phone but it soon fixed it,
- Pegasus can be installed over the wireless transceiver located near a target as well.

Targets of Pegasus Spyware

The media outlets revealed that they have found more than 1000 people in over 50 countries whose number was on Pegasus's list.

- More than 180 journalists were found on that list from organizations including New York Times, CNN, and Al Jazeera.
- according to reports, many numbers were clustered in 10 countries-, **Kazakhstan, Morocco, Rwanda, Mexico, Azerbaijan, Bahrain, Hungary, India Saudi Arabia,** and the **United Arab Emirates**,
- Various governments used Pegasus to spy on government officials, journalists, opposition politicians, activists, and others.

- An investigation also revealed that the Indian government used Pegasus to spy on around 300 people between 2017 and 2019.

Government's Stand on Pegasus Spyware

The government refused to say anything against the allegations made by the petitioners citing national security as a reason.

- The government again pled to set up its own probe. But the court rejected it.
- As per the court, such a course of action would violate the settled judicial principle against bias.
- The supreme country highlight three crucial imperatives- The right to privacy, freedom of the press, and Limits on teh usage of national security as a shield,
- The court also asked the committee to make recommendations on a policy framework on cyber security to make sure the privacy of the citizens will be protected.

NSO's Stand on Pegasus Controversy

According to NSO, its only motive was to sell Pegasus only to law enforcement and intelligence team government so that they can prevent crime and terror attacks efficiently. NSO also said, it doesn't operate the system and it has no visibility of the data. So it has no part to play in the Pegasus issue.

Pegasus Issue in India

As per a report by the New York Times on 31st January 2022, India has brought Pegasus in 2017 as a $2-billion defense package.

However, this statement has refused the claims. Additionally, the nodal agency and the Indian Computer Emergency Response Team deal with cybersecurity issues and have said nothing on this matter.

The court constituted a technical committee to examine the Pegasus controversy and to examine if the spyware had been used on Indian citizens. In May 2022, the committee placed an 'interim report ' before the court and asked for time for placing the final report.

Pegasus- Way Forward

The need for judicial oversight over surveillance systems and judicial investigation into Pegasus spyware is essential.

- The national security states with securing the smartphone of every Indian citizen rather than deploying spyware on them. Government must recognize it,
- The crucial part of the fundamental right is privacy,
- The government must take measures so that the spyware won't be misused by any intelligence institution or political party.