# 11 – 01 – 2024

**News:** Pegasus spyware

- The Pegasus spyware has once again ignited a debate on privacy and security.
- Recent reports by Amnesty International point to its utilization in targeting the phones of two prominent Indian journalists, prompting inquiries into potential government involvement.

## Pegasus spyware

- Pegasus is a spyware developed by the Israeli cyber arms firm NSO Group Technologies.
- It mainly uses exploit links, clicking on which installs Pegasus on the target'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.
- Citizen Lab which has investigated several cases of Pegasus infections showed through its research that social engineering is a very common strategy to deliver the most sophisticated spyware.
- Pegasus does so by exploiting vulnerabilities in the phone's operating systems (OS).

- Lookout, which is a cybersecurity company, had partnered with Citizen Lab to investigate Pegasus and found that it had exploited three zero-day vulnerabilities in iOS to successfully attain all the user access of the phone.
- A zero-day vulnerability is a flaw in a software or hardware that is previously unknown to the party responsible.
- An online database on spyware Pegasus' use was recently launched by Forensic Architecture, Amnesty International and Citizen Lab to document attacks against human rights defenders.

# Cybercrimes

- Cybercrime is a crime that involves a computer and a network.
- The computer may have been used to commit crime and in many cases, it is also the target. Cybercrime may threaten a person or a nation's security and financial health.

**Definition**

- Any offenses committed against individuals or groups of individuals to harm the reputation or cause physical or mental trauma through electronic means can be defined as Cybercrime. Electronic means can include but are not limited to, the use of modern telecommunication networks such as the Internet (networks including chat rooms, emails, notice boards and groups) and mobile phones (Bluetooth/SMS/MMS).

**Types of Cybercrimes**

- **Identity theft** – Identity theft is defined as theft of personnel information of an individual to avail financial services or steal the financial assets themselves.
- **Cyberterrorism**–Cyberterrorism is committed with the purpose of causing grievous harm or extortion of any kind subjected towards a person, groups of individuals, or governments.
- **Cyberbullying**–Cyberbullying is the act of intimidating, harassment, defaming, or any other form of mental degradation using electronic means or modes such as social media.
- **Hacking**–Access of information through fraudulent or unethical means is known as hacking. This is the most common form of cybercrime know to the public.
- **Defamation**–While every individual has his or her right to speech on internet platforms as well, but if their statements cross a line and harm the reputation of any individual or organization, then they can be charged with the Defamation Law.
- **Trade Secrets**–Internet organizations spend a lot of their time and money in developing software, applications, and tools and rely on Cyber Laws to protect their data and trade secrets against theft; doing which is a punishable offense.
- **Freedom of Speech**–When it comes to the internet, there is a very thin line between freedom of speech and being a cyber-offender. As freedom of speech

enables individuals to speak their mind, cyber law refrains obscenity and crassness over the web.

- **Harassment and Stalking**–Harassment and stalking are prohibited over internet platforms as well. Cyber laws protect the victims and prosecute the offender against this offense.