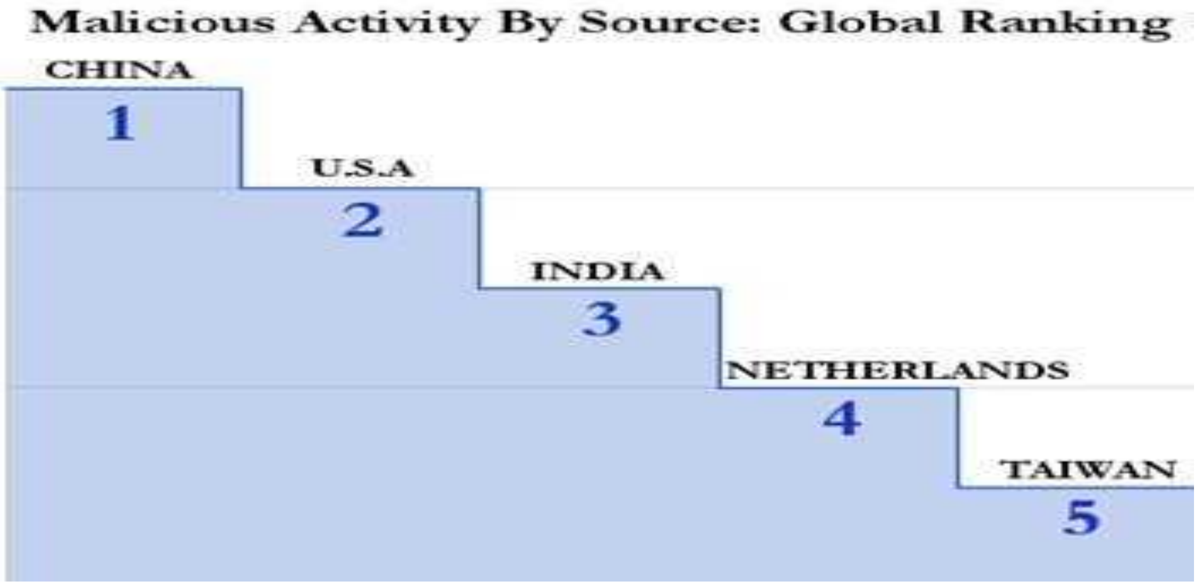
Cyber Crime

Introduction

- Everybody thinks that only stealing someone's private data is Cyber Crime. But in defining terms we can say that '**Cyber Crime refers to the use of an electronic device (computer, laptop, etc.) for stealing someone's data or trying to harm them using a computer.**
- Besides, it is an illegal activity that involves a series of issues ranging from theft to using your system or IP address as a tool for committing a crime.

- *Do you know that over the last ten years Cyber Crime rose 19 times and Cyber crime arrests are nine times in India according to NCRB data? After, U.S.A and China, India ranked third in Malicious Activity. Also, Internet Subscribers in India crossed 400 million marks and 462 million by June 2016.*



Types of Cyber Crime

Speaking in a Broadway we can say that Cyber Crime are categorized into four major types. These are **Financial, Privacy, Hacking, and Cyber Terrorism.**

- **The financial** crime they steal the money of user or account holders. Likewise, they also stole data of companies which can lead to financial crimes. Also, transactions are heavily risked because of them. Every year hackers stole lakhs and crores of rupees of businessmen and government.
- **Privacy** crime includes stealing your private data which you do not want to share with the world. Moreover, due to it, the people suffer a lot and some even commit suicide because of their data's misuse.
- In, **hacking** they intentional deface a website to cause damage or loss to the public or owner. Apart from that, they destroy or make changes in the existing websites to diminish its value.
- Modern-day terrorism has grown way beyond what it was 10-20 years ago. But **cyber terrorism** is not just related to terrorists or terrorist organizations. But to threat some person or property to the level of creating fear is also Cyber Terrorism.

Category Of Cyber Crime

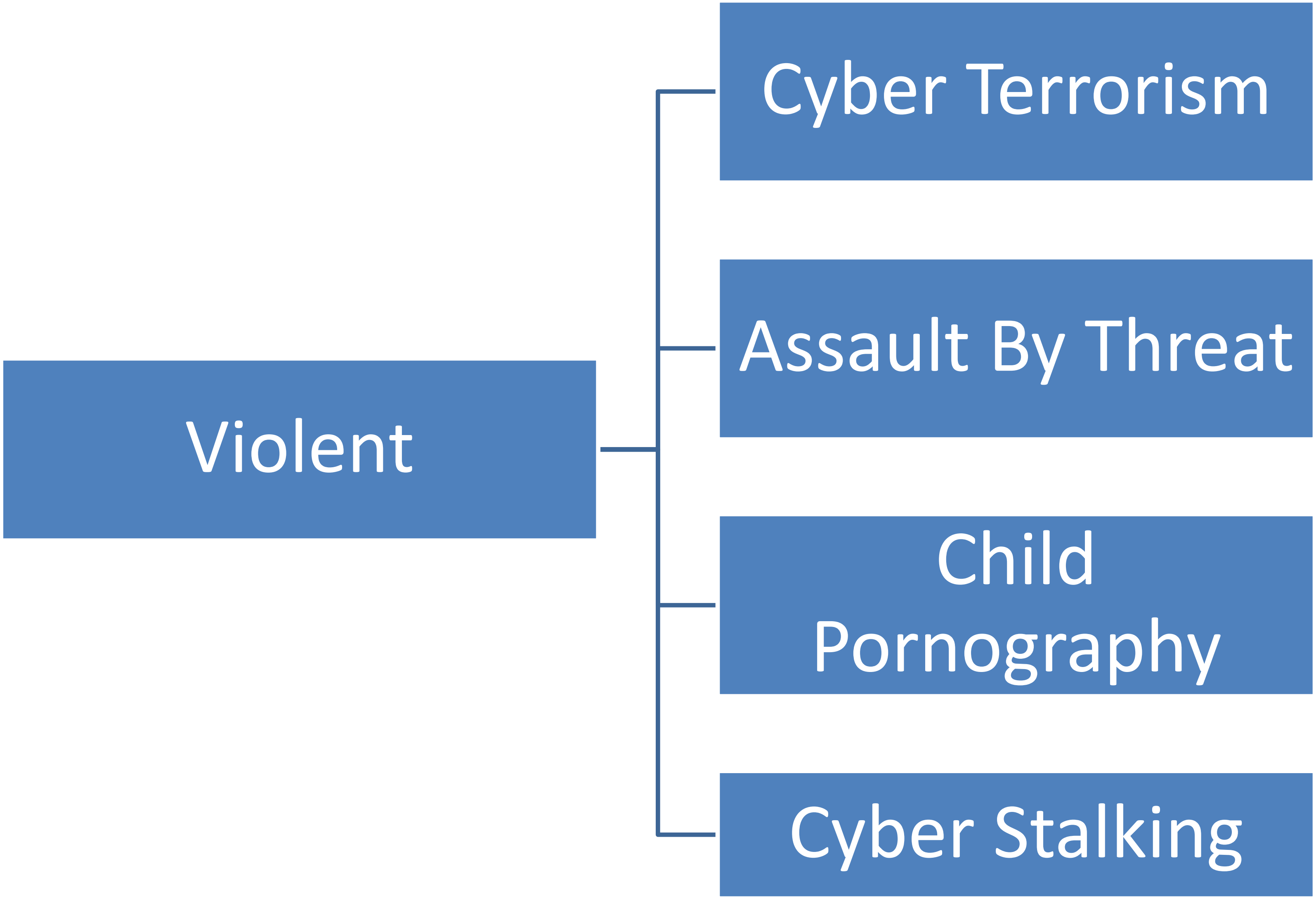
1. Violent (Potentially Violent)

- This Cyber Crime leads to Physical risk to Victims.
- This means that another person's physical body was harmed during the committing of a crime.

2. Non Violent.

- Non-violent crimes are defined as a crime where no injury or force is used on another person.
- Non-violent crimes are often measured in terms of loss to the victim or economic damage.

Categories of Violent Cyber Crime



Violent

Cyber Terrorism

Assault By Threat

Child Pornography

Cyber Stalking

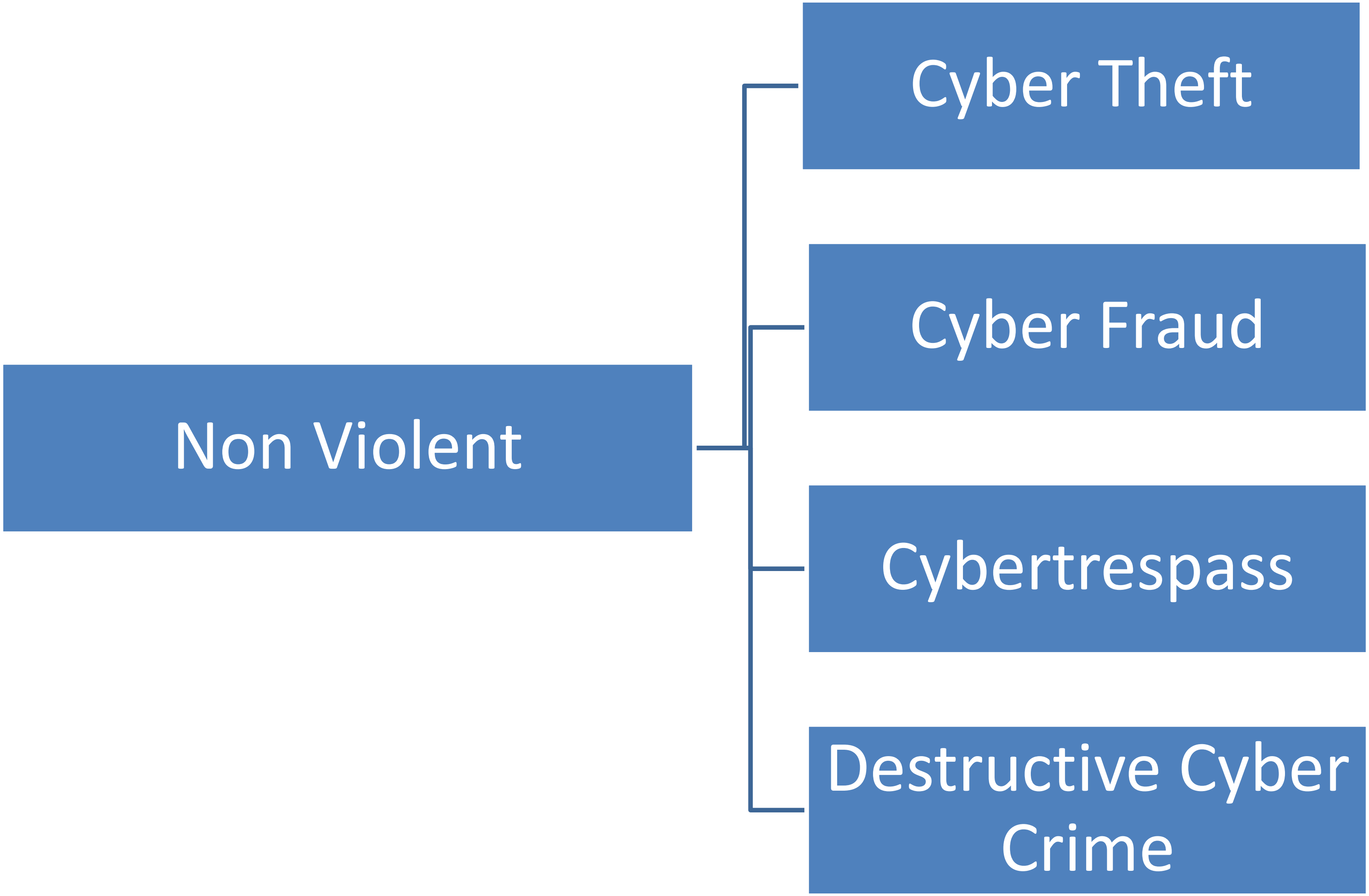
- **Cyber Terrorism :** The politically motivated use of computers and information technology to cause severe disruption or widespread fear in society. **cyberterrorism** include "attacks that lead to death or bodily injury, explosions, plane crashes, water contamination etc.

- **Assault By Threat :** A person commits Assault by Threat if he or she intentionally or knowingly threatens another person with imminent bodily injury. In this context, the term “bodily injury” means anything that causes pain, even if it does not leave a mark. The threat can be verbal or non-verbal.

- **Child Pornography :** The paedophiles sexually exploit the children either by using them as sexual objects or by taking their pornographic pictures in order to sell those over the internet.

- **Cyber Stalking:** Stalking can be termed as the repeated acts of harassment targeting the victim such as following the victim, making harassing phone calls, leaving written messages or objects. Stalking may be followed by serious violent acts such as physical harm to the victim. Cyber Stalking means repeated acts of harassment or threatening behaviour of the cyber criminal towards the victim by using internet services.

Categories of Non-Violent Cyber Crime



Non Violent

Cyber Theft

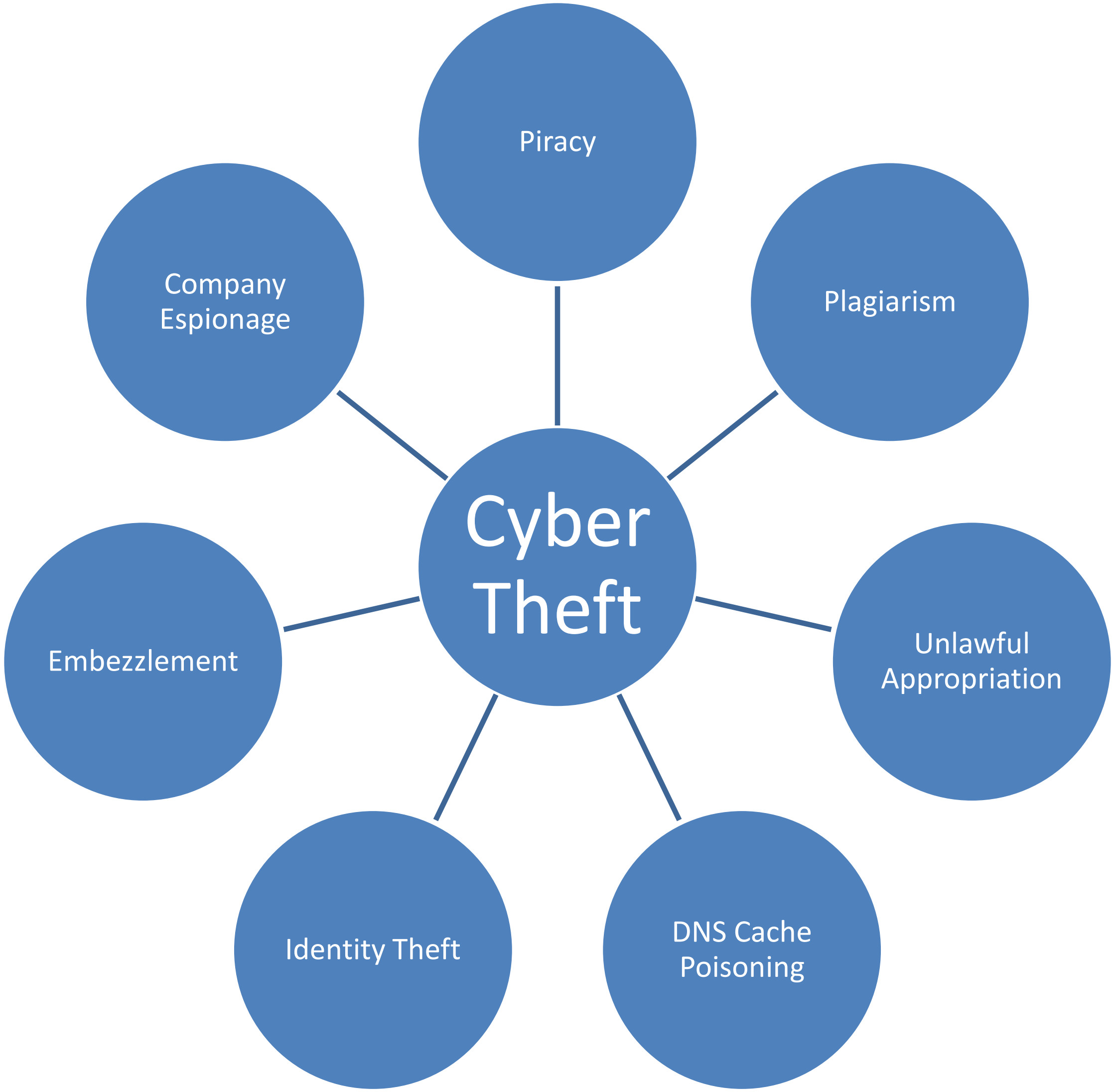
Cyber Fraud

Cybertrespass

Destructive Cyber Crime

- **Cyber Theft: Cyber theft** is a part of cybercrime which means **theft** carried out by means of computers or the Internet. The most common types of **cyber theft** include identity **theft**, password **theft**, **theft** of information, internet time **thefts** etc.
- **Cyber Fraud: Internet fraud** is a type of **fraud** or deception which makes use of the **Internet** and could involve hiding of information or providing incorrect information for the purpose of tricking victims out of money, property, and inheritance. Crime of using dishonest methods to take something valuable from another person. Eg: ATM Fraud
- **Cybertrespass:** Computer **trespass** is defined as accessing a computer without proper authorization and gaining financial information, information from a department or agency from any protected computer.
- **Destructive Cyber Crime :** Also called Destruction of Service (DeOS) These attacks are meant to cause the maximum amount of damage possible, oftentimes resulting in a loss of data, a disruption of operations and an increase in the cost of data recovery.

Cyber Theft Categories:-



Cyber Theft

Piracy

Plagiarism

Unlawful Appropriation

DNS Cache Poisoning

Identity Theft

Embezzlement

Company Espionage

- Piracy: Software **piracy** is the unauthorized use and distribution of computer software. Software developers work hard to develop these programs, and piracy curbs their ability to generate enough revenue to sustain application development.

- Plagiarism: **Plagiarism** refers to using some other person's ideas and information without acknowledging that specific person as the source. Similar to all other forms of theft, **plagiarism** also has many disadvantages associated with it.

- Unlawful Appropriation: **Appropriation** of something that belongs to someone else is the act of taking it, usually without having the right to do so.

- DNS Cache Poisoning: **DNS cache poisoning**, also known as **DNS** spoofing, is a type of **attack** that exploits vulnerabilities in the domain name system (**DNS**) to divert Internet traffic away from legitimate servers and towards fake ones.

- Identity Theft: **Identity theft**, also known as identity **fraud**, is a crime in which an imposter obtains key pieces of personally identifiable information (PII), such as Social Security or driver's license numbers, in order to impersonate someone else.

- Embezzlement: **Embezzlement,** also known as **employee theft**, is the act of someone wrongfully appropriating funds that have been entrusted to their care but which are owned by someone else.

- Company Espionage: Also called Industrial espionage is the illegal and unethical theft of business trade secrets for use by a competitor to achieve a competitive advantage. Industrial espionage is conducted by companies for commercial purposes

Thank You..