International Scholars Journals

International Journal of Law and Legal Studies ISSN 2736-1608 Vol. 10 (1), p. 001, March, 2022.
Available online at www.internationalscholarsjournals.com © International Scholars Journals

*Commentary*

# Classifications of cybercrime

**George Berman**[*]

Department of Law, Terrace University of Leeds, Leeds, UK.

Received: 01-Mar-2022, Manuscript No. IJLLS-22-60989; Editor assigned: 03-Mar-2022, PreQC No: IJLLS-22-60989(PQ); Reviewed: 18-Mar-2022, QC No: IJLLS-22-60989; Revised: 25-Mar-2022, Manuscript No: IJLLS-22-60989 (R). Published: 31-Mar-2022

## DESCRIPTION

A cybercrime is a crime undertaken by the use of computers and a network. It's possible that the computer was utilised in a criminal act or that it was the intended victim. Cybercrime can put a person's safety and financial well-being at threat. When confidential information is intercepted or disclosed, whether lawfully or illegally, there are numerous privacy concerns. On a worldwide scale, espionage, financial theft, and other cross-border crimes are perpetrated by both governmental and non-governmental actors. Cyberwarfare is a term that relates to cybercrime that takes place across frontiers and involves at least one nation-state. Cybercrime, according to Warren Buffett, is the "number one problem with mankind" that "poses genuine hazards to humanity."

### Classifications

While conventional crime is down, cybercrime is increasing on a sporadic basis over the world. From financial crimes to scams, trafficking, and ad frauds, computer crime covers a wide spectrum of activities.

**Financial fraud crimes:** Any dishonest misrepresentation of fact intended to allow another to undertake or refrain from doing anything that causes loss is referred to as computer fraud. In this case, the deception will result in an advantage for the perpetrator. Namely, by changing something without permission. Employees manipulating data before entry or entering fake data, as well as entering unauthorised instructions or performing unauthorised processes, is a typical kind of theft that requires little technical expertise. Changing, deleting, suppressing, or stealing data, frequently in order to hide illicit transactions. It's difficult to notice this. Other types of fraud, such as bank fraud, carding, identity theft, extortion, and theft of classified information, may be helped by computer systems. These types of crimes frequently result in the theft of personal or financial information.

**Cyberterrorism:** Since early 2001, government officials and information technology security experts have observed a considerable surge in Internet difficulties and server scams. The Federal Bureau of Investigation (FBI) and the Central Intelligence Agency (CIA) are growing concerned that such attacks are part of a coordinated attempt by cyberterrorist foreign intelligence services or other groups to map potential security gaps in important systems. A cyberterrorist is someone who uses a computer-based attack against computers, networks, or the information stored on them to intimidate or compel a government or an organisation into advancing his or her political or social goals.

**Cyberextortion:** When a website, e-mail server, or computer system is exposed to or threatened with repeated denial of service or other attacks by hostile hackers, this is known as cyberextortion. In exchange for money, these hackers promise to stop the attacks and provide "protection." Cybercriminal extortionists are increasingly targeting corporate websites and networks, disabling their ability to operate and demanding payments to restore service, according to the Federal Bureau of Investigation. Each month, the FBI receives more than 20 reports, with many going unreported in order to keep the victim's name out of the public eye.

**Computer as a target:** A small handful of criminals are responsible for these crimes. Unlike crimes that use computers as a tool, these crimes necessitate the offenders' technical knowledge. As a result, the nature of crime evolves in tandem with technological advancements. These crimes are relatively new, having only existed for about as long as a computer, which shows how unprepared society and the globe as a whole are to confront them. This type of crime is committed on the internet on a daily basis. It is rarely done by lone wolves; typically, big syndicate groups are involved.

[*]Corresponding author. George Berman, E-mail: george1233@gmail.com.