Sociology and Criminology: Open Access

OPEN ACCESS Freely available online

Commentary

The Study of Cybercrime and its Classification

Jane Austen*

Department of Criminology and Criminal Justice, Florida International University, Miami, USA

ABOUT THE STUDY

Cybercrime is the term used to describe a crime carried out through a computer or computer network. Either the computer was utilised in the crime or it was the intended target. Someone's security or finances may be compromised through cybercrime. There are many privacy concerns with cybercrime when private information is intercepted or made public, whether legally or unlawfully. International cybercrimes, such as financial theft, espionage, and other cross-border crimes, are committed by both state-sponsored and non-state actors. Cyberwarfare is the term sometimes used to describe cybercrimes that take place beyond national boundaries and include at least one nation-state.

Classifications

A wide range of actions, including as financial crimes, scams, cybersex trafficking, and advertising fraud, are included in the category of computer crime.

Computer fraud: The use of a computer to steal, modify, or obtain unauthorised access to a computer system or network is known as computer fraud. Internet fraud may be used to describe computer fraud that uses the Internet. Depending on the jurisdiction, computer fraud is defined legally in a variety of ways, but often entails unauthorised access to a computer. Hacking into computers to change data, disseminating dangerous software like computer viruses or worms, installing malware or spyware to steal data, phishing, and advance-fee scams are all examples of computer fraud.

Cyberterrorism: Generally speaking, cyberterrorism is an act of terrorism carried out *via* computer or cyberspace resources. Cyberterrorism can take the form of planned, widespread disruption of computer networks, particularly those of personal computers connected to the Internet, using tools such computer viruses, computer worms, phishing, malicious software, hardware techniques, or programming scripts.

Cyberextortion: Cyberextortion is a sort of extortion that happens when a website, email server, or computer system is attacked by malevolent hackers, such as through denial-of-service attacks, or is threatened with such an attack. Cyberextortionists demand money in exchange for a guarantee that the assaults will stop and that they would provide "protection". The Federal Bureau of Investigation claims that extortionists engaged in cybercrime are increasingly targeting corporate networks and websites, impairing their ability to function, and demanding payments to get their service back. Each month, the FBI receives more than 20 reports of crimes, many of which are not filed because the victim's identity should not be made public. Usually, attackers employ a distributed denial-of-service attack. There are other forms of cyberextortion, such as doxing, extortion, and bug poaching.

Cybersex trafficking: Cybersex trafficking involves the transportation of victims followed by the webcam live streaming of rape or coercive sexual activity. The victims are taken to "cybersex dens" after being threatened, tricked, or kidnapped. Anywhere the cybersex traffickers have access to a computer, tablet, or phone with an internet connection is a potential location for the dens. The perpetrators make advantage of video conferencing, dating websites, chat rooms on the internet, apps, dark web sites, and other platforms. To conceal their identities, they make use of digital currency and online payment methods. Authorities get millions of reports of its occurrence each year. To combat this kind of cybercrime, new laws and police protocols are required.

Cyberwarfare: Cyberwarfare is the use of cyber-attacks against an enemy state to disrupt critical computer systems and/or inflict damage on the level of actual warfare.

Computer as a target: These crimes are carried out by a certain set of offenders. These crimes require the offenders to have technical understanding, as opposed to crimes that use computers as a tool. Therefore, just as technology changes, so does the nature of crime. Since computers have only been around for a short while, these crimes are relatively new, which explains how unprepared society and the rest of the world are to confront them. This kind of crime is frequently performed online every day. They are typically committed by huge syndicate groups rather than lone criminals.

Computer as a tool: The computer might be viewed as the tool rather than the target when the person is the main objective of cybercrime. These crimes typically require less specialised knowledge. Usually, human shortcomings are exploited. Legal

Correspondence to: Jane Austen, Department of Criminology and Criminal Justice, Florida International University, Miami, USA, E-mail: JaneAusten12@yahoo.com

Received: 01-Mar-2022, Manuscript No. SCOA-22-20784; **Editor assigned:** 04-Mar-2022, PreQC No. SCOA -22- 20784 (PQ); **Reviewed:** 18-Mar-2022, QC No. SCOA-22-20784; **Revised:** 25-Mar-2022, Manuscript No. SCOA -22-20784 (R); **Published:** 01-Apr-2022, DOI: 10.35248/2375-4435.22.10.245

Citation: Austen J (2022) The Study of Cybercrime and its Classification. Social and Crimonol. 10: 245.

action against the versions is more challenging because the harm is primarily psychological and intangible. These are the types of crimes that have been committed for many years in the real world. Before the invention of computers and the internet, there were scams, thievery, and other similar crimes. Simply said, the same criminal has been handed a weapon that broadens their potential victim base and makes them more difficult to track down and capture.

Obscene or offensive content: For a variety of reasons, the content of websites and other electronic communications may be objectionable, obscene, or offensive. These communications can be prohibited in some situations.

Ad-fraud: Cybercriminals choose to commit ad-frauds because they are less likely to be caught and because they can be very profitable.

Online harassment: Online bullying is the repeated harm done to another person by an individual or group using information and communication technologies. This could involve making threats, embarrassing them, or humiliating them online.

Drug trafficking: Drug trafficking is a worldwide illegal business that involves the production, distribution, and sale of chemicals that are forbidden by law.