
Cybercrime
Legal Challeneges
Chain of custody
Defining cybercrimes
Varying legal systems
Emerging Trends
AI Deep Fakes
Social Engineering
IoT & Cloud vulnerabilities
Specific Cybercrimes
Phishing
Malware
Identity Theft
Online Fraud
Hacking
Exploitation and vulnerabilities
Data Breaches
Sophisticated tools
Dark Web Activities
Stolen Data Marketplaces
Drug Markets
Ransomware-as-a-service(Raas)
Targeted Victims
Individuals
Companies
Governments
Critical Infrastructures
Motives
Political
Monetary
Revenge
Hackers
Non-state actors
Black hat
Hacktivists
Leukfeldt Organized Cybercrime Typology
Type 1: Low-tech attacks with a high degree of victim-attacker interaction
Type 2: Low-tech attacks with a low degree of victim-attacker interaction
Type 3: High-tech attacks with a low degree of victim-attacker interaction
Wall's Cybercrime Typology
Cybertrespass
Cyberfraud
Cyberpornography
Cyberviolence
Criminology theories
Social Learning Theory
Rational Choice Theory
Routine Activity Theory
Legal Policies
Computer Fraud and Abuse Act (1986)
Electronic Communications Privacy Act (1986)
Identity Theft and Assumption Deterrence Act (1998)
Digital Forenics
Log Analysis
Data Recovery
Malware Analysis
Cybersecurity (Measures)
Multi-Factor Authentication
Data Backups
Encryption
Training
Enforcement & Responses
Law Enforcement Reporting (FBI/IC3)
Incident Response Plans (IRP)
International Jurisdiction

Conceptual Analysis

Cybercrime occurs every day around the globe, impacting how people, businesses, and governments operate and respond to digital threats. It is also a broad subject that numerous scholars and enforcement agencies study to gain an understanding of how criminals use computers or anything digital to do things with malicious intent. By understanding tactics and motives, we can connect as to how to further prevent these crimes from happening, and this also demonstrates how technology can be weaponized if put into the wrong hands. Wall's cybercrime topology is the key topology used in cybercrime literature and gives an insight into cybercrime through four categories such as cyber trespass, cyberfraud, cyberpornography, and cyberviolence. These four categories represent the different approaches that cybercriminals use to exploit individuals, systems, and digital environments. In addition, it contributes to a more structured way to understand cybercriminal behavior and makes it easier to analyze, address, and study across the contexts of social, legal, and technological.

A couple of key relationships (shown in green arrows) and current events (shown in red arrows) that I've identified are the connections between motives and the criminology theories; targeted victims and specific cybercrimes; emerging trends and specific cybercrimes; and digital forensics and legal challenges. Criminology theories such as Social Learning, Rational Choice, and Routine Activity provide a background explanation for cybercriminal behavior and how they gain their motives. For example, the routine activity is the theory that involves a motivated offender, a target, and an absent guardian. How this theory correlates with motives is that cybercriminals look for opportunities to exploit a system or individual for personal gain. Targeted Victims, such as individuals, companies, governments, and critical infrastructures, are the most susceptible to cybercrimes, such as those listed in the map, due to human error and system vulnerabilities. As for current events, cybercriminals have become stealthier in their attacks, which leads to the emerging trends such as AI deep fakes, social engineering, and the exploitation of IoT and cloud vulnerabilities. From the current cybercrimes (listed as specific), these emerging trends further enhance the effectiveness of each attack, leading to loss of data and systems. In digital forensics, it faces legal challenges such as the chain of custody. If the evidence is slightly tampered with or has improper storage, it becomes inadmissible in court, meaning that the evidence wouldn't be of any use for the case presented and would lead to further legal consequences. One surprising discovery is that this broad subject could be broken down into 15 categories, and within these categories, some of these correlate well with each other, as in connections.

Process Reflection

In the making of this concept map, I felt like one of those investigators trying to piece together evidence on those wooden boards. However, this helped me to break down a broad topic into main topics that are usually associated with it. I didn't know that some of these main topics could connect greatly, as well as their subtopics connecting with other subtopics. The software I've used to create the map was MindMeister. This made the organization easier, and the concept map aesthetically pleasing to the eye. Some challenges that I had were figuring out what other topics coincide with the central topic of cybercrime and making connections to each topic, which ChatGPT helped with. I also had trouble

organizing each topic because the words and lines were overlapping, and I wasn't familiar with the software. However, with a lot of clicking around and messing with the tool, I was able to organize the topics. Overall, I had fun creating the concept map and also learning about how these topics connect. A few skills I've gained from this final project were critical thinking, concept mapping, and identifying relationships with topics.

AI Disclaimer

In the process of making this concept map project, ChatGPT was used for brainstorming a few connections between the main topics. I was able to upload my map, and it gave me ideas on how to connect them.