Katie Barnes

MET CJ 610 01

Professor Lee

May 13, 2021

The Concepts of Computer Crime Cybercrime

As technology evolves computer crimes have grown and include many new types of crimes, which encompasses a wide range of crimes defined as cyber-crimes (Choi, Lee, Louderback, 2019). The most recent definition of cybercrime during the Fourth Industrial Revolution is “any illegal behavior directed by means of electronic operations that target the security of computer systems and the data processed by them” (Choi, Lee, Louderback, 2019). Computer crime is a component of cybercrime, but computer crime is not necessarily a cybercrime (Module 1, 2021). The differences between Cybercrime and Computer crimes fall into separate categories. Cybercrime involves Cyber-stalking, Cyber-harassment, Cyber-pornography, and Cyber-violence while Computer Crime is more Cyber-trespassing and Cyber-deception and theft (Module 1, 2021).

One of the biggest problems for analysis of cybercrime is the absence of a consistent current definition, even among law enforcement agencies (Yar, 2005). Since the term has no specific referent in law… consequently, the term might best be seen to signify a range of illicit activities whose common denominator is the central role played by networks of information and communications technology (ICT) in their commission (Yar,2005). For agencies to find a commonplace approach and further classify cybercrime agencies would need to distinguish between ‘computer-assisted crimes such as fraud, theft, money laundering, sexual harassment, hate speech, pornography and ‘computer-focused crimes’ like hacking, virtual attacks, and website defacement (Yar, 2005). One classification, which cybercrime can be subdivided is the way the technology plays a role, i.e., whether it is a contingent ('computer-assisted') or necessary ('computer-focused') element in the commission of the offence (Yar, 2005). According to Yar (2005), David Wall subdivides cybercrime into four categories:

1. Cyber- *trespass* - crossing boundaries into other people's property and/or causing damage, e.g., hacking, defacement, viruses.
2. Cyber-*deceptions* and *thefts* – stealing (money, property), e.g., credit card fraud, intellectual property violations (a.k.a 'piracy').
3. Cyber-*pornography* - activities that breach laws on obscenity and decency.
4. Cyber-*Violence* – doing psychological harm to, or inciting physical harm against others, thereby breaching laws pertaining to the protection of the person, e.g., hate speech, stalking.

   According to Choi, Lee & Louderback, the National White Collar Crime Center defines a computer crime as a violation involving a computer. Computer crimes include targeting the content of computer operating systems, programs, or networks (hereafter referred to as "computer systems"), typically involving one or more of the following:

   (a) Accessing computer systems without permission (unauthorized access)

   (b) Damaging computer systems (sabotage)

   (c) Acquiring information stored on computer systems – without permission (theft of data)

   (d) Acquiring services from computer systems- without permission (theft of services).

Using the computer as a tool to commit a computer crime or cybercrime is one of the same but how a court of law processes the actual laws makes a difference in sentencing and how the legal aspects or the crimes come together.

Thus, knowing how to classify the differences between cybercrime and computer crime is imperative within the criminal justice system. “Cybercrimes have new dimensions to illegality and violent threats that law enforcement officials and policymakers struggle to address (Dolliver, 2013)”. The damage that can be caused by a person or small group over the world wide web can cause as much damage as it once took an entire army to cause’ even worse the offender does not have to physically be anywhere near the victim/s (Dolliver, 2013). Since a crime can be committed anywhere over the internet it can be extremely challenging for law enforcement to trace or connect the dots as to who is committing the crimes. The offender could be anywhere all over the world thousands of miles away or continents away (Dolliver, 2013). There are Networks over the internet that host services using special software like the Darknet which criminals can access through what is called a TOR browser. Many Darknet patrons use Tor software to remain anonymous online (ROCIC, 2013). The Tor browser is used for both good and bad but what is worrisome for law enforcement and other government agencies is the fact that there are predators on the Darknet such as pedophiles, hitmen, drug dealers and weapon traffickers and that is only to name a few (ROCIC, 2013). Since the Tor is legal it cannot be illegal for the average joe for regular use since there are no laws against it. There is currently no ban placed on the anonymity of the Tor browser as there are no laws against freely using a Tor browser. As I stated before, the Darknet is used for many things both good and bad. Moreover, the TOR browser for an example is for the government and the army to share top secret information. This is the reason why cybercrime is extremely challenging and complex. However, as cybercrime continues to evolve and expand cybersecurity intelligence is expanding as well.

References

Choi, K. Lee, H. (2021). Module 1 *Introduction and Overview of Cybercrime* [Lecture PDF]. MET CJ 610 01: Cybercrime (2021 Summer 1) Retrieved from https://onlinecampus.bu.edu.

Choi, K. Lee, H. Louderback, E. (2019). *Historical Evolutions of Cybercrime: From Computer Crime to Cybercrime.* [Lecture PDF]. MET CJ 610 01: Cybercrime (2021 Summer 1) Retrieved from https://onlinecampus.bu.edu.

Dolliver, D.S. (2013). SSN Basic Facts. *How Cybercrimes Challenge Law*. Retrieved from https://scholars.org/contribution/how-cybercrimes-challenge-law-enforcement

Graham, R. Smith, S. (2020). Cybercrime and Digital Deviance. *Understanding Cybercrime in the Digital Environment*. Routledge. New York, New York

ROCIC. (2013). Penetrating the Darknet. *Silk Road, Bitcoins, and the Onion Router*. Retrieved from https://www.vanderbilt.edu/olli/class-materials/Pentrating_the_Darknet.pdf.

Yar. M (2005). The Novelty of 'Cybercrime'. *An Assessment in Light of Routine Activity Theory.*

Retrieved from DOI: 101177/147737080556056 https://heinonline-org.ezproxy.bu.edu/HOL/Page?handle=hein.journals/eujcrim2&id=390&collection=journals&index=