Investigative Report: Cybercrimes

Charles B. Rodgers
School of Criminal Justice
CRJU 3309: Cyber Crime
Dr. Misty Ladd
October 6, 2022

Investigative Report: Cybercrimes

Cybercrime, an epidemic that encompasses every aspect of our lives, from social to financial our presence in the cyberscape can be touched by Cybercrime. To understand the reasoning behind Cybercrime we must look at many different factors that affect the perpetrators. In the realm of Criminal Justice, the medium is the only difference between 'terrestrial' and Cybercrime. This close distinction between real and online allows for models to be made to predict certain types of Cybercrimes based on trends. Since the Justice landscape has had time to test the "How?" and "Why?", cybercrimes are not the mystery they once were twenty years ago.

What are the major reasons for cybercrimes?

Majid Yar and Kevin F. Steinmetz (Cybercrime and Society, 2019) break down the distinctions of Cybercrime as it pertains to an individual or to an entity such as a company or government. These distinctions also play into the psychology behind the motives that Cybercrimes are committed. For an individual, the motives are, for the most part, straightforward. If an individual is the target of cybercrime, Yar and Steinmetz (2019) give some examples of this targeting. Theft of computer resources (p.60), to pirate software or mine cryptocurrency, Theft of proprietary or confidential information (p.60-61), this is to steal banking information or even medical documentation, and the malicious target of Systems sabotaging, alteration and destruction (p.61), this is to install malware to track the individual or even destroy the system entirely. The motive toward the individual heavily leans toward financial gain, yet there are also hints of several theories behind what drives these motives.

For Cybercrime, I find that there are three main theories that genuinely encapsulate the niche of cybercrime more than regular crime theories towards the individual. Yar and Steinmetz (2019) lend their research in presenting the theories of the; Social learning theory, Strain theory, and Drift and neutralization theory. The Social Learning Theory (p.28-30) coined by Edwin H.

Sutherland (1939) and refined by Ronald Akers and Robert L. Burgess (1966), emphasizes that an individual, such as a child, is susceptible to the behavior of those around them and are prone to imitate such behavior if no adverse consequences present themselves (Akers and Jensen, 2006). Sixty years ago when this theory was formed individuals were formed by other individuals around them, today individuals are formed by the media and the influences thereof they surround themselves in. Since cybercrime is not properly defined for youths, cybercrime in its most basic forms is fostered among this demographic. This theory can attribute to the trend of internet doxxing that is involved with online gaming. The Strain theory delves deeper into the motives of younger generations being susceptible to cybercrime. These strains are caused both online and offline, through cyber and real bullying, financial woes, and general societal pressures. Robert Agnew (1992) combined the existing Strain theory with one that incorporated more of a criminal sect. Agnew (1992) attributes these criminal tendencies to negative emotions fostered by the Strain. These emotions, if not checked, would later cause an individual to lean towards criminal tendencies. In today's world, it is easier for those under this strain to express their negative emotions due to the access that the internet enables a person with. This theory can attribute to cybercrimes such as doxxing, piracy, and the theft of financial keys. Drift and Neutralization theory as they pertain to cybercrime, dictate that the individual ‘drifts’ towards cybercrime as an escape from their upbringing, and they neutralize their involvement by blaming ignorance or denying the instance in its entirety. This theory can be attributed to the sudden emergence of piracy, since it as cybercrime is the least intuitive. Cybercrime toward the individual can be theorized with these theories provided by Yar and Steinmetz (2019), yet since we humans are such unpredictable creatures it is hard to exactly pinpoint every cause for cybercrime toward an individual.

Cybercrime and how it pertains to an entity is an easier-defined beast than that of the individual. In certain instances, the theories that are compared with individuals can be used but hackers usually make their motives known when committing crimes against an entity. Crimes against entities can be broken down into three categories, Hacktivism, Cyberterrorism, and Individualism. Per Checkpoint.com Hacktivism is "hacktivism is the act of hacking, or breaking into a computer system, for politically or socially motivated purposes." Hacktivism at its core, within a grey area, is a form of protest. Legal? No, hence is why it is in my paper about Cybercrime. Per Yar and Steinmetz (2019) Hacktivism can be seen as a virtual sit-in (p.85), Website defacements (p.86), and even in extreme cases a virus that displays a message (p.87). These methods of protest are seen as cybercrime due to their intrusion into certain systems that would otherwise be prohibited by outside sources. Cyberterrorism is a different beast than that of Hacktivism. Per TechTarget, Cyberterrrorism is "often defined as any premeditated, politically motivated attack against information systems, programs, and data that threatens violence or results in violence. The definition is sometimes expanded to include any cyber attack that intimidates or generates fear in the target population." The most recent and notable cyberterrorist attack would be the Colonial Pipeline hack in May 2021. This attack targeted a key weakness in US government infrastructure to shut off gas supplies to the entire East coast under the guise of ransomware. Cyberterrorism also takes place when a hostile foreign government or entity attempts to steal anything from classified information, disrupt local services, or even steal cryptocurrency from firms. The final perpetrators of attacks against entities are the individuals. Individualism is quite common in the inner circles of hackers with each trying to outdo the last. Yar and Steinmetz (2019) in the opening of their book reference the 'Love Bug' virus that caused over $10 billion in damages in 2000, this 'bug' was developed by just one person. Individualism

towards entities usually stems from a stigma against the organization, trying to get said organization's attention, or just to display their prowess against a larger body than that of another individual. The Individual is more unpredictable than that of another organization, due to motives cannot be tracked easily by what outliers would usually flag a person for.

How do we fight Cybercrimes?

Cybercrime may feel like an overpowering foe, that is akin to the mythical beast hydra, you cut off one head two grow in its place. While in certain instances the fight is definitely a hard-fought battle, fighting Cybercrime is possible. Before going into any battle or competition research on the adversary is done. The same is done for Cybercrime, through the form of Predictive Analytics. Shannon Flynn from makeusof.com defines Predictive Analytics as a way to “compare a business’s security measures and cybercrime trends among similar companies. They can then show how cybercriminals may attack them and where the holes in their defenses are.” From Flynn’s definition, this allows companies in multiple industries to assess past attacks against competitors and look for the same weaknesses in their business. Flynn also states that these predictive models can subvert attacks before they happen with machine learning that enables AI to learn the common causes. With the vast scope of Cybercrime, predictive analytics alone cannot slow the epidemic that is this crime. To stop Cybercrimes against the individual, we put our trust in anti-virus software, VPNs, and the built-in security features of sites and browsers. There are many legal and official ways to stop Cybercrime against the entity, through laws, triple-A protection, and even physical means. Two tangible examples would be; RIAA is the anti-piracy law passed to stop the copy and distribution of copyrighted material, and “Trespassing in Government Cyberspace (18 U.S.C. 1030(a)(3))” prohibits any unauthorized persons from using any government computer for its specific purpose. Even though these laws

get broken, they are in place to deter hackers from committing Cybercrime. Cybercrime is an ever-present danger in our lives and the ecosystem we live in, but as technology progresses the more we evolve to combat this danger.

References

Yar, M., & Steinmetz, K. F. (2020). *Cybercrime and society*. MTM.

Jnguyen. (2022, May 11). *What is hacktivism?* Check Point Software. Retrieved October 5, 2022, from https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-hacktivism/#:~:text=Derived%20from%20combining%20the%20words,said%20to%20be%20a%20hacktivist.

Sheldon, R., & Hanna, K. T. (2022, January 19). *What is cyberterrorism?* SearchSecurity. Retrieved October 5, 2022, from https://www.techtarget.com/searchsecurity/definition/cyberterrorism

Flynn, S. (2022, January 29). *How predictive analytics can combat cybercrime*. MUO. Retrieved October 5, 2022, from https://www.makeuseof.com/predictive-analytics-combat-cybercrime/#:~:text=Predictive%20analytics%20models%20can%20compare,holes%20in%20their%20defenses%20are.

About piracy. RIAA. (n.d.). Retrieved October 5, 2022, from https://www.riaa.com/resources-learning/about-piracy/#:~:text=(Title%2017%2C%20United%20States%20Code,%2C%20Sections%20501%20and%20506).&text=Making%20unauthorized%20copies%20of%20copyrighted,thousands%20of%20dollars%20in%20damages.

Congressional Research Service. (2014, October 15). *Cybercrime: An overview of the Federal Computer Fraud and abuse statute and Related Federal Criminal Laws*. EveryCRSReport.com. Retrieved October 5, 2022, from https://www.everycrsreport.com/reports/97-1025.html#_Toc401151140