Analyzing Criminological Theories and Their Relativity to Cybercrime

Nicolas R. Stephens

Department of Sociology and Criminal Justice, Old Dominion University

Professor Raelee Passuello

CRJS 215S: Introduction to Criminal Justice

16 September 2025

Analyzing Criminological Theories and Their Relativity to Cybercrime

Cybercrime is estimated to cost the world 13.82 trillion dollars by 2028 (Golombick, 2025). If cybercrime were a country, its Gross Domestic Product (GDP) would rank it well above Germany, placing it the third-largest economy in the world, behind only the United States and China. Cybercrime has even become more lucrative than drug trafficking, but there is one major issue: transnational cybercrime is almost impossible to successfully prosecute. The primary reason why transnational cybercrime is often difficult to prosecute lies in one word: jurisdiction. Jurisdiction refers to the legal operational area over which a government entity has control. Therefore, when it comes to transnational cybercrime, governments typically lack jurisdiction over other sovereign nations. The process is further complicated when the cyber-attack originates from adversary nations (i.e., nations not allied or on diplomatic terms with the target). For example, America is not legally allowed to send federal agents into China to arrest members of prolific state-sponsored hacking groups, such as APT 41; however, nations can employ other tactics to achieve the same result. Such tactics can include, but are not limited to: sanctions on nation-states and/or specific hacker groups, offering high financial incentives for information and/or assistance leading to arrest, seizing website domain names, and asset seizure. The use of these tactics differs significantly from those used to arrest and prosecute cases of traditional street crime like murder, rape, robbery, aggravated assault, arson, and so on. In cases involving traditional street crime, local or sometimes state and federal law enforcement agencies collaborate to locate the perpetrator of the crime and gather sufficient evidence to convict them in a court of law, ensuring due process. During criminal cases, lawyers often have access to widely accepted and established definitions of crime, which enable them to prosecute based on the specifics outlined in the law. However, in the context of cybercrime, there is no universal

definition of committing criminal acts, which makes tracking and prosecuting criminal activity even more challenging. Definitions of cybercrime often vary across organizations within the same country and differ significantly across national borders, so one could imagine the complexity that a lack of a universal definition creates while trying to prosecute cybercriminals on a global scale. As the threat of cybercrime rises exponentially each year, it is essential to understand how many cybercriminals are successfully prosecuted annually. This excerpt from Leyden et al. (2025) examines some statistics behind cybercrime prosecution:

> 300,000 people were victimized over the Internet to the tune of $1.1 billion. Although that averages out to only $3,666 per victim, the typical Internet hacker commits thousands to hundreds of thousands of these crimes and almost never gets caught. Those who get nabbed are unlikely to spend any time in jail, and when they do, they'll probably serve, at most, a few years in a low-security facility. (para. 5)

Leyden and his colleagues go on to write:

> According to FBI's 2010 Internet Crime Report, from 303,809 complaints, 1,420 prepared criminal cases resulted in a mere six convictions. That's one jailed cyber criminal for every 50,635 victims, and these are just the cases significant enough to be reported to the FBI. (para. 7)

Although this report utilizes information from the 2010 FBI Internet Crime Report, the information remains relevant today, as cybersecurity threats continue to evolve and protections against them often lag behind. Researchers and cybersecurity professionals are left playing catch-up with cybercriminals, whose ever-evolving methods make it increasingly harder to prosecute. Although the technology around cybercrime remains new, one aspect that remains

constant, like every other type of crime, is the human element. Therefore, we can apply a criminological lens to examine the roots of why cybercriminals commit cybercrime. By examining cybercrime through the lens of the Classical School of criminological thought, it becomes apparent that cybercriminals are free-thinking and rational beings who are fully aware of the harm they cause to people worldwide. Cybercrime is a complex and highly technical phenomenon, with attacks that can last for years. This means that cybercriminals are aware of the consequences of their actions, yet they often choose to cause harm to others primarily for financial gain. However, if cybercrime is examined through a Positivist lens, then cybercriminals commit cybercrime because they are genetically predisposed to commit delinquent acts. Some cybercriminals could exhibit signs of being antisocial, reclusive, impulsive, egotistical, or even be exposed to poor socioeconomic conditions, which triggers a latent biochemical reaction in their brain that pushes them along the path towards criminality. It should be noted that positivist thought doesn't revolve entirely around genetics, but rather encompasses a broad range of factors, including socioeconomic factors, as mentioned earlier. Deterrence also plays a role in the way cybercriminals operate. On the topic of deterrence from criminal activity, Schram and Tibbetts (2020) state, "three characteristics of punishment make a significant difference in whether an individual will commit a criminal act —in other words, they deter crime. These vital deterrent characteristics of punishment include celerity (swiftness), certainty, and severity." The first characteristic is celerity, or the swiftness of the punishment. Beccaria, the creator of these three elements of deterrence, can be quoted as saying, "the more promptly and the more closely punishment follows upon the commission of a crime, the more just and useful will it be." However, in the realm of cybercrime punishments, if at all, they take months or potentially years to be handed out, so cybercriminals aren't deterred from committing cybercrime because, if they

do get punished, they know it will be a long, drawn-out process and they will be more psychologically detached from the punishment the longer they go without receiving said punishment, which means they are likely to commit the same crime again. This is contrary to regular street crime, as criminals know they will most likely be caught before the end of the week, or, depending on the crime, possibly within a month. The speed of their punishment often resonates in their brain, which leads them to seek a better life without committing a crime. The second element of deterrence, which is arguably the most important, is certainty. Certainty revolves around the idea that some offenders commit a crime because they have a low chance of getting caught, which is most likely the greatest reason that a majority of cybercriminals commit the crimes they do. Based on the statistics earlier, most hackers are likely to evade law enforcement, which allows them to commit more serious cybercrimes with almost zero risk to themselves or those around them. In regard to regular street crime, this is not the case, as you are almost certain to get caught if you commit certain crimes like murder, arson, armed robbery, felonious assault, etc., the list goes on. The third and final element of deterrence is severity, which refers to the severity of the punishment for the given crime. Since cybercrime is relatively new in comparison to more traditional methods of crime, this aspect is certainly lacking in today's society. One might think that stricter punishments for committing certain cybercrimes could help reduce the crime rate, but for this to be effective, it would need to work in conjunction with the other two methods. Looking at more traditional crime, though, it is relatively clear that severity alone doesn't help reduce crime rates. If such were the case, most rational individuals wouldn't commit murder in certain states because it could lead to the death penalty. Although there are certain differences, deterrence still works in the same way in the cyber environment; however, the methods used to catch cybercriminals need to evolve so that the most important

aspects of deterrence can be effectively implemented to reduce the cybercrime rate. As methods for catching cybercriminals evolve, so too should the understanding of the psychological and biosocial risk factors associated with them. As previously stated, criminality is a complex interplay of genetic predisposition and socioeconomic factors. To prevent the creation of more cybercriminals, policies should be in place to flag certain behaviors and provide rehabilitation to affected individuals. If an individual exhibits signs of antisocial disorder along with high technological expertise, there is a heightened risk for that individual to be a cybercriminal, but rehabilitation doesn't always work, so there should also be practices in place that aim to direct affected individuals towards hacking with ethical intent, or hacking in regard to a professional career and/or military service.

In conclusion, by examining cybercrime through a criminological lens, the effectiveness of certain actions against cybercriminals can be made clear, and allow for updates to policies and tactics used to catch cybercriminals. However, it also allows for transparency regarding the difficulties of measuring and prosecuting cybercrime, as well as the steps to make the process more effective in protecting a future dominated by technology.

References

Golombick, C. (2025, September 7). *Cyberattack costs in 2025: Statistics, trends, and real examples*. ExpressVPN. https://www.expressvpn.com/blog/the-true-cost-of-cyber-attacks-in-2024-and-beyond/

Leyden, J., Events, S. O. for C., Violino, B., & Staff, C. (2025, September 11). *Why internet crime goes unpunished*. CSO Online. https://www.csoonline.com/article/548638/cyber-crime-why-internet-crime-goes-unpunished.html

Schram, P. J., & Tibbetts, S. G. (2020). Introduction to Criminology: Why do they do it? (3rd ed.). SAGE Publications, Inc.