Cybercrime from an Interdisciplinary Perspective

Aiden E. Payne

Old Dominion University

IDS 300W: Interdisciplinary Theory and Concepts

Dr. Constance Merriman

October 15, 2024

Abstract

What makes people choose to commit cyber crime over traditional crime? And how is it that cybercrime has become so popular in recent years? These are a few questions that are prevalent in society today and need answers as society grows increasingly reliant upon the internet for its daily interactions. Through the use of interdisciplinary research we can tackle these questions from multiple angles to get the best understanding of a complex question that has no one right or wrong answer. Through research people will find that there are many aspects from multiple perspectives of life that contribute to people committing cybercrime. Criminological, sociological, and technicological are the three main disciplinary perspectives that this paper will cover the causes and questions surrounding cybercrime. Each one of these plays an important role in understanding why cybercrime has become such an issue in today's society. This paper aims at breaking down each discipline so that the reader may understand at a deeper level what exactly the perspective of each discipline is and how they can work together to explain why people commit cybercrime.

Introduction

With the internet advancing over the last 20 years remarkable technological advancements have been made that have allowed us to have access to the internet which is the world's largest information system. With these freedoms of the internet there has also become an increase in cybercrime. Cybercrime has grown in recent years and is now one of the world's top mediums of crime. With this in mind the questions arise: What has led to cybercrime becoming so popular and what has led criminals to choose it over traditional crime? There is no one reason as to why cybercrime persists, many factors play a key role in why millions of cybercriminals continue to terrorize the internet today. Due to the way cybercrime affects many different aspects and sectors of life it is important to view the causes of cybercrime through an interdisciplinary lens. Cybercrime is unique as it literally affects everyone with internet access and therefore affects all of society.

Just like traditional in person crime there is no real reason as to why people might choose to commit crime. With cybercrime the idea remains the same in that there is no one reason to engage in it. With the understanding that there are many different reasons for why someone might choose to commit cybercrime, it is important to look at the causes from an interdisciplinary perspective to get the strongest understanding of what might be leading to increasing rates of cybercrime. Breaking down cybercrime into different aspects and interdisciplinary approaches allows us to examine cybercrime from different angles and cross examine the causes to come to a final understanding of the topic. This helps us to reach an unbiased conclusion while covering the most bases of cybercrime. Applying various disciplinary

perspectives such as: sociology, criminological, economic, and legislative, we can receive a deeper understanding of why people commit cybercrime and hopefully mitigate it in the future.

Cybercrime and Disciplinary Perspectives:

First off, what is cybercrime? According to Cisco, cybercrime is an illegal activity that involves the internet and computers (What is cybercrime?). With this in mind it is important to view cybercrime through the lens of various disciplinary perspectives as crime is at the very fundamentals of cybercrime. The criminological perspective on cybercrime insists that many different reasons play a role in why someone might commit a cybercrime. Criminology does this by using different theories to understand what makes people choose to commit crime in the first place. Criminology is a very interdisciplinary field to begin with as many of the theories that make criminology up contain backgrounds from sociology, economics, technological, and legislation. Most criminological theories tend to target the who,why, and how questions pertaining to motivations behind crime. These reasons are very important when looking at cybercrime because most criminological theories apply to cybercrime as they do to traditional crime. Theories like deterrence theory and routine activities theory which originated from traditional crime are just as much applicable to cybercrime as they are traditional crime.

The idea behind Routine Activities Theory is that "for a crime to occur, three necessary elements must converge in time and space: likely offenders, suitable targets, and the absence of capable guardians."(Routine Activity Theory**)** this perfectly gets along with criminology as the suitable target happens to be anyone using the internet, this is what differs cybercrime from traditional crime in that anyone can be a victim not just a present vulnerable target. Motivated offender can be anyone who uses the internet as well, this could be someone motivated by

money, revenge, or political reasons. The lack of a suitable guardian is huge as there are no police officers patrolling the internet and there are minute amounts of laws put in place to deter people from committing cybercrime. The time and place at which people converge is amplified with cybercrime due to people being able to interact with people at any time of the day from anywhere in the world. Routine Activities Theory explains why cybercrime occurs and it explains why cybercrime is growing at an alarming rate. The freedom to access any suitable target at any suitable time without the fear of being caught due to anonymity online as well as little to no laws against cybercrime shows us just how the perspective of criminology allows us to see how and why cybercrime occurs.

Another theory from the criminological discipline that can help us to understand cybercrime through its perspective is the deterrence theory. The main idea behind deterrence theory is that severe punishments and lack of opportunity deter people from committing a crime. This is applicable to cybercrime because it can show us why cybercrime is so popular. Through this perspective we can see that cybercrime is so popular due to little to no deterrents on the internet. Most of the internet isn't properly monitored for cybercrime and people can easily bypass evidence with various ways of maintaining their anonymity. Criminological discipline gives us a fundamental understanding of why crime happens through various theories. We can apply these theories to cybercrime and see why it is so popular due to the way the internet amplifies the opportunity for cybercrime to occur. The criminological perspective builds off of the sociological perspective as it takes ideas from various disciplines and converts them into theories.

The sociological perspective aims at tackling the why behind cybercrime through the understanding of how we as humans interact with other humans within society on the internet.

This perspective can include sub disciplines like economics which tend to be a key reason behind why cybercrime is so popular. With the entirety of society interacting with one another through the internet it makes the sociological perspective on cybercrime invaluable. With the very foundations of our society being built upon the internet the sociological discipline helps us to get a unique perspective on why cybercrime occurs at the base level. This perspective helps us look at the why and who of cybercrime.

Reasons why cybercrime occurs and is rampant today can be explained through a sociological perspective as we look at how society has evolved over the last 10 years. A large societal change that took place in 2019 would be the COVID-19 pandemic which affected everyone around the world. According to researchers “the onset of the COVID-19 pandemic, more internet users worldwide have become dependent on the internet in all areas, including education, financial transactions, and working from home [4]. During this dependency, damage from cybercrimes has steadily increased [5,6].”(Understanding cybercrime from a criminal's perspective: Why and how suspects commit cybercrimes?) This massive societal change caused an increase in cybercrime due to the amount of people using the internet. The suitable targets on the internet increased immensely as people were forced to use the internet as a means of banking, work, and school. Just how much did COVID-19 affect cybercrime? “It was reported by the FBI that 791,790 cybercrime complaints resulting in more than US$4.1 billion losses were received by the Internet Crime Complaint Centre in 2020 and that number of reported cases has increased 69 percent compared to the reported cases in 2019.”(A systematic literature review on cybercrime legislation) this shows us just how much the societal changes brought with COVID-19 affected the growth of cybercrime for the worse.

Another source of cybercrime brought up by the societal perspective would be the relation between higher socioeconomic status and likelihood to commit cybercrime. People socioeconomic status has been recorded to show patterns amongst cybercrime “Specifically, a higher income, more education, a lower poverty rate, and a higher inequality are likely to make the Internet penetration be more positively related with cybercrime perpetrators”(The Economics of Cybercrime: The Role of Broadband and Socioeconomic Status) the reason behind thai si that higher education and lower poverty rate can directly be related to a person's internet connection and having more tools at their disposal. This societal perspective can help us lead to an understanding of what exactly allows individuals to commit crime and how we can monitor these high speed connections better than what we currently are. This perspective allows us to see what events in our daily lives have caused cybercrime to be such an issue. The unique perspectives the sociological discipline brings to the table allows for cybercrime to be more understandable as it is explained in a way that is relatable to our daily lives and interactions. Within the societal perspective the idea pertaining to higher internet speeds playing a role in cybercrime would also relate to the technological side of things as the internet is the platform where cybercrime takes place.

The technological perspective is the foundation upon which the societal and criminological perspectives are built. Through the technological discipline we can understand cybercrime at the fundamental level and understand how it might be conducted as well as how we can mitigate it as well. Because of the lack of face to face interaction in cybercrime, it is important to understand how cybercrime occurs. On the larger scale with banks and governments there are regularly cybercriminals trying to break in ,however; on the day to day basis most cybercrime attacks tend to be caused by people clicking on malicious links or falling victim to

social engineering. From the technological perspective we can get a brief understanding of the methods cyber criminals use to commit crimes so that we can get a better understanding of how to not fall victim to cybercrime.

The technological perspective plays an important role in the spread of cybercrime as well as the mitigation of it. How has technology contributed to the growth of cybercrime? According to researchers “Cybercrime is growing and current technical models to tackle cybercrime are inefficient in stemming the increase in cybercrime. This serves to indicate that further preventive strategies are required in order to reduce cybercrime.”(Cybercrime classification and characteristics) The main reason as to why cybercrime exists from a technological perspective is how there isn't enough anti-cybercrime technology available yet. This is similar to criminological deterrence theory which also explains cybercrime based on lack of deterrences. The internet for the most part is a free space in that people may search wherever on the internet they may choose. This can lead to an infinite number of ways and targets that cybercriminals can attack. With that being said the technological advancements are also being used by cybercriminals for malice. Things like automation and bots have allowed cybercriminals to complete tasks and attacks in no time due to them having all of the internet at their disposal. With the growth technology has seen in recent years and the growth of people using that technology it is easy to see a parallel between technology and cybercrime. With this in mind we can see just how cybercrime is understood through the lens of the technological discipline. Cybercriminals are given a plethora of information and suitable targets all while not having to leave their home. The automation and anonymity that the internet provides makes cybercrime a clear winner over traditional crime in terms why a criminal would choose it.

Using the 10-step research process we can deeper analyze these perspectives by cross examining the sources and their perspectives. All three of these disciplines have their own unique perspective as to why cybercrime occurs and why people have chosen it over traditional crime. These disciplines all tend to overlap on the idea that cybercrime has increased as more and more people have started to use the internet for their daily lives. All disciplines point to the idea that there is simply more opportunity for criminals on the internet with little to no risk of getting caught. These disciplines tend to agree on what mainly causes crime but the hierarchy of how they rank the causes tends to be different. The criminological perspective displays the cause of cybercrime through various theories which are derived from a mix of societal, psychological, and economic factors. The societal perspective examines cybercrime as the result of various societal changes in the last 10 years, similarly to criminology ,however; the societal perspective highlights how there are simply more users or suitable targets on the internet which leads to an increase in cybercrime. Where societal and criminological perspectives both share ideas around human interaction and behaviors, the technological perspective aims at discovering the reasoning for cybercrime through how technology has given criminals a new means of crime. Using the 10-step research process we can see how the perspectives differ from one another and how they share similarities with one another. This allows us to gather pieces of information and compare and contrast to help us find a clear result that is shared by multiple disciplines while also understanding their own unique approaches to how and why people commit cybercrime.

Conclusion:

The interdisciplinary perspectives show that cybercrime does not have one singular cause but a multitude of causes. Each perspective provides a unique understanding of what cybercrime

is and how it relates to that perspective. All disciplinary perspectives elucidate how the low risk of getting caught matched with a large number of suitable targets makes the internet a prime choice to commit crime rather than traditional in person crime. With this in mind it is important for society to properly train themselves in proper cyber hygiene and using the internet with caution. It is also important that adequate legislation is put in place to ensure that people are deterred from committing cybercrime and if they do commit crime then they will be charged accordingly. Cybercrime is a huge issue in society and will remain so if proper actions are not taken to further understand its causes and produce solutions.

References

Khan, Shereen, et al. “A Systematic Literature Review on Cybercrime Legislation .” *F1000Research*, F1000 Research Limited, 23 Aug. 2022, f1000research.com/articles/11-971.

Park, Jiyong, et al. “The Economics of Cybercrime: The Role of Broadband and Socioeconomic Status: ACM Transactions on Management Information Systems: Vol 10, No 4.” *ACM Transactions on Management Information Systems*, 5 Dec. 2019,

Hamid Jahankhani, and AbstractOver the last two decades. “Cybercrime Classification and Characteristics.” *Cyber Crime and Cyber Terrorism Investigator's Handbook*, Syngress, 25 July 2014, www.sciencedirect.com/science/article/pii/B9780128007433000128#bi0010.

Harjinder Singh Lallie a, et al. “Cyber Security in the Age of Covid-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks during the Pandemic.” *Computers & Security*, Elsevier Advanced Technology, 3 Mar. 2021, www.sciencedirect.com/science/article/pii/S0167404821000729?casa_token=bW4SEnvUbMMAAAAA%3Aop74Iw-Uwgew9CT3LDjj7-PAfCrgtDRGJkK3kwQJ-1XUyZMGX3A1BbN8gjB1VVcLlosUeogjag.

Miró, F. (n.d.). *Routine activity theory - miró - - major reference works - wiley online library*. Wiley Online Library. https://onlinelibrary.wiley.com/doi/full/10.1002/9781118517390.wbetc198

So-Hyun Lee, et al. “Understanding Cybercrime from a Criminal’s Perspective: Why and How Suspects Commit Cybercrimes?” *Technology in Society*, Pergamon, 15 Sept. 2023, www.sciencedirect.com/science/article/abs/pii/S0160791X23001665.

What is cybercrime?. Cisco. (2024, August 27). https://www.cisco.com/site/us/en/learn/topics/security/what-is-cybercrime.html