A Current and Increasing Problem of Anti-Social Behavior via Anonymity Using Electronic Mediums Demanding Recognition as a Biopsychosocial Disorder that Perpetuates Criminal Behavior Online

Hannah Wood Despres

Follow this and additional works at: https://epublications.regis.edu/theses

Part of the Criminology Commons, Criminology and Criminal Justice Commons, Social Control, Law, Crime, and Deviance Commons, and the Social Psychology Commons

Recommended Citation
https://epublications.regis.edu/theses/839

This Thesis - Open Access is brought to you for free and open access by ePublications at Regis University. It has been accepted for inclusion in All Regis University Theses by an authorized administrator of ePublications at Regis University. For more information, please contact epublications@regis.edu.
A CURRENT AND INCREASING PROBLEM OF ASOCIAL BEHAVIOR VIA ANONYMITY USING ELECTRONIC MEDIUMS DEMANDING RECOGNITION AS A BIOPSYCHOSOCIAL DISORDER THAT PERPETUATES CRIMINAL BEHAVIOR ONLINE

by

Hannah Wood Despres

A Thesis/Capstone Proposal Presented in Partial Fulfillment of the Requirements for the Degree Masters of Criminology

REGIS UNIVERSITY

October 2017
A CURRENT AND INCREASING PROBLEM OF ANTI-SOCIAL BEHAVIOR VIA ANONYMITY USING ELECTRONIC MEDIUMS DEMANDING RECOGNITION AS A BIOPSYCHOSOCIAL DISORDER THAT PERPETUATES CRIMINAL BEHAVIOR ONLINE

by

Hannah Wood Despres

Has been approved

October 2017

APPROVED:

__John Giduck____________, Faculty Facilitator
__James Ponzi ____________, Thesis Advisor
__Vincent Wincelowicz______, Faculty Chair
ABSTRACT

Most people who commit crime fall into a classification of criminological, sociological or psychological disorders called biopsychosocial disorders. Cyber-crime is unique in the fact that, cyber criminals can commit crimes behind completely closed doors and they are virtually anonymous. This makes for a varied environment of theory on the causation of cyber-crimes. The proposed disorder theory, computer mediated anonymity asocial disordered theory, is based on the notion that the anonymous nature of electronic mediums in communication has significantly changed people’s interpersonal skills. The change in interpersonal development is therefore affecting social engagement behavior online and has allowed a lack of moral accountability, leading to an increase in cyber-crime.

Keywords: biopsychosocial theories, cyber criminals, inclusion of Computer Mediated Anonymity Disorder Theory
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABSTRACT</td>
<td>3</td>
</tr>
<tr>
<td>INTRODUCTION</td>
<td>5</td>
</tr>
<tr>
<td>LITERATURE REVIEW</td>
<td>5</td>
</tr>
<tr>
<td>CURRENT THEORIES</td>
<td>8</td>
</tr>
<tr>
<td>Routine Activities Theory (RAT)</td>
<td>8</td>
</tr>
<tr>
<td>Deterrence Theory</td>
<td>9</td>
</tr>
<tr>
<td>Social Learning</td>
<td>10</td>
</tr>
<tr>
<td>ANONYMITY</td>
<td>13</td>
</tr>
<tr>
<td>COMPUTER MEDIATED ANONYMITY ASOCIAL DISORDER THEORY</td>
<td>15</td>
</tr>
<tr>
<td>CONCLUSION</td>
<td>16</td>
</tr>
<tr>
<td>REFERENCES</td>
<td>17</td>
</tr>
</tbody>
</table>
INTRODUCTION

Criminal behavior is typically explained by one of the biopsychosocial theories. For example, when someone commits a crime out of severe emotional distress or anger, it could fall under Strain Theory (Criminological), Social Learning Theory (Psychological) or Deterrence Theory (Sociological). Current accepted biopsychosocial disorder theories do not encompass cyber-crime and anonymity, but rather seek to stage it as a social disorder often caused by a stressor or phobia or set of events that induces the criminal behavior. A new disorder theory of causation is important to establish to appropriately strategize a defense against the increase of online crime. The disorder theory is unique due to its inclusion of the anonymous nature of the electronic medium. This paper will not seek to identify causes that have previously been identified such as motivations for crime (financial gain, anger, biological traits), but will seek to identify a new classification of a biopsychosocial disorder theory that is separate from the other established ones.

Looking at different psychological, criminological and sociological disorder theories shows that not one of them categorizes the problem of anonymity when engaging online effectively. Developing a sound theory, inclusive of the nature of anonymity and its direct link to the increase of online crime, will help to identify one cause and its implications on the increasing problem of cyber-crime. In identifying this disorder’s characteristics, society will develop a better understanding of one of the attributes of increasing online crimes.

LITERATURE REVIEW

Before the internet’s capabilities criminals were never able to access one another with such ease and anonymity as they can today. The increase of crimes committed online is growing
at a steady pace according to the FBI’s Internet Crime Complaint Center. The FBI’s ICCC reported that there were 8,910 reported victims of identity theft in 2014 as compared to 16,385 reported victims in 2016, 5,017 victims of harassment online in 2014 as compared to 16,385 in 2016 and 9,715 of online extortion in 2014 as compared to 17,146 victims in 2016 (FBI ICCC, 2014 & 2016).

When looking at the reasons most research falls back on theories in psychology, sociology and criminology, it is because these theories focus on criminal behavior caused by a stressor, biology, compulsions, phobias or a set of events. Mark Rogers, CISSP, writes that these theories are generally accepted as sound theories and attempted to apply these theories to the “behavior of hackers”. However, the article does not discuss anonymity, and instead reflects on current accepted theories “hackers” could belong in. The article also focuses on the behavior of hackers, not necessarily anyone who commits crime online.

In looking at the current research involving the increase of cyber-crime due to anonymity, there is a lack of biopsychosocial disorders specific to the nature of anonymity and the increase of cyber-crime. One analysis discusses the nature of groups engaged in cybercrime and briefly touches on the fact that some people commit crimes based on the sense of anonymity, “...in others, a sense of impunity (born of over-confidence in anonymity) is apparent.” (Broadhurst, Grabosky, Alazab, Bouhours & Chon, 2014).

Other such examples may be cases of cyber bullying or online harassment in where the person was not likely to bully or harass someone face to face, but ended up being involved in it online. One study on the impact of face to face engagement as compared to electronic communication showed that when no electronic device was a medium to communication, the subjects showed a higher level of empathy and concern as compared to those that used electronic
mediums (Misra et al., 2014). A similar study found that electronic devices affected human relationships with one another, and went as far to state that the devices used as mediums negatively impacted relationships in the areas of closeness and communication quality, especially during personally significant subjects (Przybylski and Weinstein, 2012).

These examples show why people are more prone to commit crimes under the veil of anonymity. The effect of electronic communication and anonymity has led to a decline of our social engagement and development of interpersonal skills that uphold bonds to our community and define our moral, ethical and legal accountability. One study analyzed youth engaged in the cyber world and the effects that growing up with electronic devices in every aspect of their world has had on these youths. Their conclusion found that it had significantly decreased the youths’ face-to-face interactions. The researchers also concluded that these youths may very well experience a significant life impact regarding the underdevelopment of their interpersonal skills and their “presentation of self” (Brignall & van Valey, 2005).

Another article by Kimberly Christopherson (2007) shows the literature regarding anonymous communication online and the social psychological theory to explain the behaviors. It asserts that there are theoretical explanations for behaviors occurring specifically due to the nature of anonymity online. It discusses negative and positive factors of being anonymous during computer mediated communication. Christopherson discusses Deindividuation Theory, which contends that individuals lack self-awareness in groups, and Adaptive Structuration Theory which analyzes the formation of group structures and their influence on communication and decision making. However, it falls short of linking the behavior to cyber-crime (Christopherson, 2007).
Lastly, a literature review done by Armstrong and Forde (2003) link the anonymous nature to the perpetuation of online crime, proposing a greater need for balance between freedom of speech, privacy and law enforcement. A seemingly simple solution would be to eliminate or restrict anonymity online. However, this is a complex area, and a thorough discussion regarding the right to privacy and free speech, with the conflicting consideration of the victimization of others and what those amendments protect or cannot protect, would need to take place.

CURRENT THEORIES

Routine Activities Theory (RAT)

RAT is a criminological theory developed in 1979 by Marcus Felson and Lawrence Cohen, which focuses on characteristics of a crime, rather than the offender. RAT proposes that three aspects of a crime must be present: (1) a person must be motivated to commit an offense, (2) availability of a victim must exist, and (3) the element of protection/prevention must not exist. So, in summary, if there is the will, a way and no deterrent, a crime will be committed. (Cohen & Felson, 1979). This could explain why someone may commit a crime online, especially considering the anonymous nature of online interaction. The element of protection/prevention could be low in many cases and dependent on the skill level of the criminal. Take for example a scam email, a scammer could ping multiple emails with a fraudulent email asking for funding and may receive a response from 2 in 10 emails. Those 2 would be considered “unprotected” and create an opportunity. There are a considerable number of available victims when online and if a person has begun engaging in a criminal act online, the motivation is proven to exist.
The issue with this theory is that although it does explain some motivating characteristics, it does not explain why cyber-crime has increased and does not address cyber-criminal specific characteristics. It begins to, by discussing motivation of a crime being dependent on a protection/prevention of the crime, but does not elaborate. This notion however is explained in more detail when looking at Deterrence Theory which will be addressed later.

RAT is different from other criminological theories since it deals with why people commit crimes (characteristic of a crime), instead of how the criminal event is instigated (behavior of criminal). Basically, it deals with motivation characteristics for committing crime. Cyber-crime comes with a plethora of motivations, whether there is a protection/prevention measure to it, so this notion seems to fail in theorizing characteristics of cyber-crime. This theory is looking from a different perspective, and although its glance touches on some motivation of cyber-crime, it does not see it from the correct angle. Looking at cyber-crime from a behavioral perspective (of the criminal) is beneficial because it helps to understand the characteristics of the cyber-criminal. Understanding the prevalence of cyber-criminal characteristics will lead to an understanding of the increase of cyber-crime.

Deterrence Theory

Deterrence Theory is one of the oldest sociological theories that is still used today. The roots of this theory can be traced back to the mid 1600’s from three prominent philosophers, Thomas Hobbes, Cesare Beccaria and Jeremy Bentham. The ideologies of these three philosophers still exists in the modern deterrence theory. Deterrence Theory proposes that people choose whether to commit a crime based on their perception of the risks or rewards. If the reward is high and the risk is low, a person would be likely to commit a crime. If the reward was low and the risk
was high, they would likely not commit the crime. Many modern criminal justice agencies have used this theory, and continue to along with Evidenced Based Practices (EBP). EBP is a practice of deterrence based on connecting with an individual using certain techniques and helping them to address dynamic factors to prevent further criminal actions. EBP focuses on using motivational interviewing, which is a practice of active listening, accountability and empathy/sympathy. It involves a skilled use of communication and interpersonal skills in connecting with an offender.

This theory could account for motivating behaviors of committing online crime due to the anonymous nature, a person may perceive a low risk and therefore commit more crimes when online under the veil of anonymity. However, this does not explain the increase, also it would not be possible to apply the deterrent action of EBP, because when online you lack connection with people. Therefore, you would not be able to actively listen, empathize or hold an offender accountable unless they were convicted or self-incriminated. It is not just society that creates a deterrent though, it is also a person’s morality, ethics and foundational behavior that can be a deterrent. This is the foundation for social learning theory.

Social Learning

Social Learning Theory is a psychological theory that was developed in 1977 by Albert Bandura. Bandura focused on the behavioral theories of classical and operant conditioning and proposed the addition of two ideas: (1) mediating processes occur between stimuli & responses and (2) behavior is learned from the environment through the process of observational learning (McLeod, 2016). In summary, the theory proposes that when the child learns by observation and it’s reinforced by society (either negatively or positively), the adult is likely to imitate that behavior later. It is not just monkey see, monkey do, but a higher process of cognition in which
the adult, shaped as a child by adult models and societal reinforcement, thinks about the relationship between their actions and the consequences. This can explain why people commit any crimes but is broad in nature and does not explain the increase of cyber-crime. It does however explain more relating to electronic mediated communication. Children today are exposed to a far greater amount of technology and electronic mediums. As they see their role models engage in this, they mimic the social boundaries of what’s appropriate communication. Often, people are in a situation where they could be verbally communicating with one another and are instead on some electronic device. They may even be communicating with another person, rather than the one in front of them. What does this do to our interpersonal skill development? A study published by journal Developmental Psychology took 3, 461 North American girls ages 8-12 and examined the relationship between social well-being and face-to-face communication. They found that when using electronic mediums for typical communications, “negative social well-being was positively associated with levels of uses of media that are centrally about interpersonal interaction (e.g., phone, online communication) as well as uses of media that are not (e.g., video, music, and reading).” (Pea, et al, 2012). If humans lack interpersonal skills development and the opportunity to connect with the physical community around them, there

**Asocial and Antisocial Behaviors**

According to Merriam-Webster the definition of asocial is “rejecting or lacking the capacity for social interaction”. The medical definitions are “(a) not involving or taking part in social interaction with others [and] (b) hostile or harmful to organized society.” (asocial, 2017).

Antisocial is defined as “(1) averse to the society of others [and] (b) hostile or harmful to
organized society; especially: being or marked by behavior deviating sharply from the social norm. (antisocial, 2017). Daniel Bayne reviews empirical evidence on antisocial behavior online, and links online behavior to those of mob mentality models. The models state that when people are in groups that promote antisocial, asocial and deviant behaviors, an individual gets lost in the group and lose their own self-awareness and their ability to regulate their behavior. In one such study the results show that those in a group participating online, displayed more antisocial behaviors than those of individuals that were not grouped. The individuals were higher in succeeding then those in the group due to the collaboration and agreement in the group, the individuals only had themselves to decide and answered accordingly, the group was swayed by the consensus. “The mix of group identity and individual anonymity that characterizes most online communities inevitably breeds the antisocial behaviors that have become synonymous with the internet.” (Bayne, n.d.) This shows that a lack of interpersonal skill development creates asocial and antisocial behaviors, and that the anonymous nature of being online, perpetuates antisocial behaviors.

Other research theories

Many professionals have stated there is minimal research on the topic of cyber criminals regarding psychological crime theories. “Interpersonal behavior has been studied in various areas of criminal psychology for some time, although there has been relatively little research to date regarding the interpersonal skills of hackers.” (Kirwan & Power, 2013). Relevant research includes Lieberman’s questionnaire on social avoidance. The study disproved the stereotype of the lone hacker, who was socially inept and incapable of social interaction. The study found that
hackers had normal relationships (romantically speaking) and sex lives. (Lieberman, 2003 as cited in Fotinger and Ziegler, 2004). Woo (2004) conducted a study with similar results that indicate hackers do not fit previous stereotypes and are members of complex social online networks. However, Chesebro and Bonsall (1989) conducted a study suggesting that hackers consider their computers as an extension of self, and even regard their computer as a friend. So, they may be a part of extensive social networks on line, but it is not in the same way one would engage with another person in the physical world. When we engage in the physical world we gain a sense of self from interactions with another creating a foundation of interpersonal skills, as stated above in Pea, et al (2012). In contrast, according to Chesebro and Bonsall’s “avoid social communications” and Turkle (1984) suggested in her study that when people are online, they do not have a sense of self, but view the computer as an extension of self. This still does not replace the face to face interactions that are necessary to develop interpersonal skills.

ANONYMITY

Anonymity and cyber-crime is a new arena of research. There are several theories on crime however, none that really address the issue of cyber-crime, particularly the steady increase of it. Rogers and Baggili (2009) point out, most research on cyber-crime has focused on “computer science-centric programs, and little experimental research has been performed on the psychology of cyber-crime.”

Rogers and Baggili (2009) conducted an experimental study by which participant’s self-reported their involvement in “cyber-crime” behavior. The participants were divided into three
groups with “varying degrees of anonymity”. The results showed that when the groups had a higher degree of anonymity, they were more likely to self-report cyber-crime behaviors.

Another study by Adam Joinson found that the veil of anonymity emboldened participants to self-disclose a significantly higher amount of information than when face to face, or even when on a computer camera (Joinson, 2001). This is explained by looking at what computer mediated communication does to our interpersonal and social skill levels. There are many studies that conclude that excessive internet use has negative impacts. The APA defines this by the disorder of Generalized Problematic Internet Use. Taking this disorder and complimenting research on social skills and self-presentation was done by Scott Caplan (2005).

Caplan tested the hypothesis that individuals who had a lack of self-presentation skills preferred computer mediated communication, which in turn fostered more computer mediated communication, leading to compulsive internet use and the negative outcomes of such. When we engage in mediated communication we do not continue to develop interpersonal skills. Examples of interpersonal skills would be: speaking confidently by using eye contact, the ability to read someone’s inflection and tone, non-verbal cues, and the ability to empathize genuinely. When we lack interpersonal development, we tend to feel less connected to those we are interacting with, particularly online. As mentioned previously in this paper, when communicating online individuals have a decreased ability to use empathy. This constant, mediated communication is detaching us from the world around us. This is ironic since the computer seemingly connects us more to the world. A new friend in Europe, instant information on people and places thousands of miles away, and the knowledge of what is happening in our world at any moment.
In reality, we are becoming more and more disconnected the more “connected” we are. This is true in the realm of cyber-crime and is part of the causation of its increase. In fact, cyber criminals have made a market out of it. The ability to prey on people online comes with great ease, due in part to the offender’s anonymity. Millions of people use computer mediated communication every minute, all around the world. The constant mediation of communication has developed a lack of interpersonal development, thereby contributing to the increase of cyber-crime. Gone are the days of leaving your house to play and coming home when the “lights” came on. Adolescents were playing, socializing, learning and developing interpersonal skills. Now, we are texting, gaming, emailing and snapchatting, all while sitting next to people we could be conversing with face to face. Having a medium involved constantly in our connection to one another. It seems to provide a connection to the medium instead, which does not develop foundational interpersonal skill building. While individuals may not commit crimes physically, such as stealing, they may not see it the same while they are anonymous because they have not developed interpersonal skills due to the dependence on mediated communication.

COMPUTER MEDIATED ANONYMITY ASOCIAL DISORDER THEORY

The excessive use of computer mediated communication has caused individuals to lack foundational interpersonal skill development. Due to the nature of this inadequacy, paired with the dependency of computer use and the anonymity of the use, individuals are more likely to engage in criminal behavior online. I propose this accounts in part, for the increase of cyber-crimes. It’s appropriate to develop a disorder theory based on the anonymous nature of computer assisted crime because the ability to gain empirically validated data is extremely difficult.
Finding cyber criminals as participants for research would be almost impossible. However, creating a disorder, would help in gaining statistical evidence on how the use of computer mediated communication is contributing to a lack of interpersonal skills, whereby those individuals are creating an increase in cyber-crime. If agencies are able to use this information to form ideologies, policies and laws around this knowledge, then we may be able to add to our defense of becoming cyber victims. Intervening during foundational interpersonal skill development could be key.

CONCLUSION

Research in the fields of psychology, sociology and criminology lead us to the understanding that there are different motivations for criminal behaviors. However, not one of them adequately addresses criminal behavior online. Other research also indicates that the excessive and growing use of computer mediated communication is having a significant impact on how people are connected to the world around them, regarding an interpersonal skill development. Lack of interpersonal skill development, due to excessive computer mediated communication is causing a lack of empathy, self-control and ability to connect to the community. As our technology dependence grows so does our cyber-crime rate, due to the anonymous nature and lack of interpersonal communication. Creating a biopsychosocial disorder linking anonymity, computer mediated communication and the rise in cyber-crime is imperative in helping to combat its steady growth. Without proper intervention in the development of an individual’s interpersonal skills, paired with our exceeding dependence on technology and the ability to be anonymous, cyber-crime will continue to expand exponentially.
REFERENCES


