

Masthead Logo

Nova Southeastern University
NSUWorks

CEC Theses and Dissertations

College of Engineering and Computing

2019

A Psychosocial Behavioral Attribution Model: Examining the Relationship Between the “Dark Triad” and Cyber-Criminal Behaviors Impacting Social Networking Sites

Kim Withers

Nova Southeastern University, kw954@mynsu.nova.edu

This document is a product of extensive research conducted at the Nova Southeastern University [College of Engineering and Computing](#). For more information on research and degree programs at the NSU College of Engineering and Computing, please click [here](#).

Follow this and additional works at: https://nsuworks.nova.edu/gscis_etd

Part of the [Computer Sciences Commons](#)

Share Feedback About This Item

NSUWorks Citation

Kim Withers. 2019. *A Psychosocial Behavioral Attribution Model: Examining the Relationship Between the “Dark Triad” and Cyber-Criminal Behaviors Impacting Social Networking Sites*. Doctoral dissertation. Nova Southeastern University. Retrieved from NSUWorks, College of Engineering and Computing. (1072)
https://nsuworks.nova.edu/gscis_etd/1072.

This Dissertation is brought to you by the College of Engineering and Computing at NSUWorks. It has been accepted for inclusion in CEC Theses and Dissertations by an authorized administrator of NSUWorks. For more information, please contact nsuworks@nova.edu.

A Psychosocial Behavioral Attribution Model: Examining the Relationship Between the “Dark Triad” and Cyber-Criminal Behaviors Impacting Social Networking Sites

by

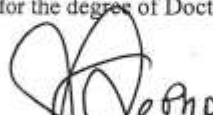
Kim L. Withers

A dissertation submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy
in
Information Systems

College of Engineering and Computing
Nova Southeastern University

2019


We hereby certify that this dissertation, submitted by Kim L. Withers, conforms to acceptable standards and is fully adequate in scope and quality to fulfill the dissertation requirements for the degree of Doctor of Philosophy.


James L. Parrish, Ph.D.
Chairperson of Dissertation Committee

3/13/2019
Date



Timothy J. Ellis, Ph.D.
Dissertation Committee Member

13 MAR 2019
Date


James N. Smith, Ph.D.
Dissertation Committee Member

13 March 2019
Date

Approved:


Meline Kevorkian, Ed.D.
Interim Dean, College of Engineering and Computing

3/13/2019
Date

College of Engineering and Computing
Nova Southeastern University

2019

An Abstract of a Dissertation Submitted to Nova Southeastern University
in Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy
A Psychosocial Behavioral Attribution Model: Examining the Relationship Between the “Dark Triad” and Cyber-Criminal Behaviors Impacting Social Networking Sites

by
Kim L. Withers
June 2019

This study proposes that individual personality characteristics and behavioral triggering effects come together to motivate online victimization. It draws from psychology’s current understanding of personality traits, attribution theory, and criminological research. This study combines the current computer deviancy and hacker taxonomies with that of the Dark Triad model of personality mapping. Each computer deviant behavior is identified by its distinct dimensions of cyber-criminal behavior (e.g., unethical hacking, cyberbullying, cyberstalking, and identity theft) and analyzed against the Dark Triad personality factors (i.e., narcissism, Machiavellianism, and psychopathy). The goal of this study is to explore whether there are significant relationships among the Dark Triad personality traits and specific cyber-criminal behaviors within social network sites (SNSs).

The study targets offensive security engineers and computer deviants from specific hacker conferences and from websites that discuss or promote computer deviant behavior (e.g., hacking). Additional sampling is taken from a general population of SNS users. Using a snowball sampling method, 235 subjects completed an anonymous, self-report survey that includes items measuring computer deviance, personality traits, and demographics. Results yield that there was no significant relationship between Dark Triad and cyber-criminal behaviors defined in the perceived hypotheses.

The final chapter of the study summarizes the results and discusses the mechanisms potentially underlying the findings. In the context of achieving the latter objective, exploratory analyses are incorporated and partly relied upon. It also includes a discussion concerning the implications of the findings in terms of providing theoretical insights on the Dark Triad traits and cyber-criminal behaviors more generally.

Acknowledgments

First, I give honor to God; without him this would not be possible. There are many people that have earned my gratitude for their contribution to my time in graduate school. More specifically, I would like to thank four groups of people, without whom this thesis would not have been possible: my thesis committee members, my colleagues, and my family.

My Advisor

First, I am indebted to my advisor, Dr. James L. Parrish. Since first taking me under his tutelage, Dr. Parrish believed in me like nobody else and gave me endless support. He has pushed me to think without guidance and make choices on my own. He also has taught me not to overthink everything and to just breathe. On the academic level, Dr. Parrish taught me fundamentals of conducting research in the information systems area. Under his supervision, I learned how to define a research problem, find a solution to it, and finally publish the results. On a personal level, Dr. Parrish inspired me and at the same time kept me smiling through the pain by his humorous and passionate attitude. To summarize, I would give Dr. Parrish most of the credit for my becoming the researcher I am today.

Committee Members

Along with my advisor, I would like to thank the rest of my dissertation committee members – Dr. Timothy Ellis and Dr. James Smith – for their great support and invaluable advice. I am thankful to Dr. Ellis, an expert in his field, for his crucial, but worthy remarks that shaped my dissertation proposal defense. I am also grateful to Dr. Ellis for his insightful comments and for sharing with me his tremendous experience in co-authoring research articles. I am quite appreciative of Dr. Smith for agreeing to serve on my dissertation committee on such short notice without hesitation. I also show the utmost gratitude for his expertise in PLS-SEM data analysis techniques and passing on the knowledge that he learned from some of the best scholars.

Colleagues

I also extend thanks to my boss, Joseph Harten, for whom I have the utmost love and respect. Since the day I joined his team, he has done a great deal for me. Joe has always supported my educational endeavors and continues to inspire me to push forward, no matter the hardships. Joe has been a boss and a true friend, and I will never forget his faith in me to be the best I can be. And to all my other team members who have weathered this nocturnal storm with me.

Family and Friends

Last but not least, I would like to express my deepest gratitude to my parents, family, and friends. This dissertation would not have been possible without their warm love, continued patience, and endless support. I thank Pastor Mel, Minister Ethel and Myra Roberson for continued prayers. To Dr. Freddie Hartfield, my college math professor, who always believed in me. I also want to dedicate this dissertation to my family who have transitioned to Heaven: Mary Murray, Edward D. Murray, Jewel F. Ireland, Cleo Murray, Larry D. Murray. May they know that I honor their memory in all that I do. To Darryl Willis, I miss you. May heaven know your worth.

Abstract	iii
Acknowledgements	iv
List of Tables	viii
List of Figures	ix

Chapters

1. Introduction	1
1.1 Background	1
1.2 Problem Statement	6
1.3 Dissertation Goals	9
1.4 Research Question	10
1.5 Importance and Relevance of Research	10
1.6 Barriers and Issues	13
1.7 Assumptions, Limitations, Delimitations	15
1.7.1 Assumptions	15
1.7.2 Limitations	16
1.8 Definitions of Key Terms	18
1.9 Summary	20
2. Literature Review	22
2.1 Introduction	22
2.2 “The Dark Triad”	23
2.3 Cyber Crime	29
2.4 Criminal Behaviors	32
2.4.1 Unethical Hacking	36
2.4.2 Cyberstalking	39
2.4.3 Cyberbullying	41
2.4.4 Identity Theft	44
2.5 Theoretical Framing	46
2.5.1 Attribution Theory	47

2.5.2 Conceptual Model	50
2.5.3 Hypotheses	51
2.6 Summary	53
3. Methodology	54
3.1 Introduction	54
3.2 Research Design	54
3.3 Survey Sample and Procedures	55
3.4 Measurement Model	58
3.4.1 Independent Constructs	58
3.4.2 Dependent Constructs	59
3.4.3 Factorial Validity Assessment	61
3.4.4 Discriminant Validity Assessment	62
3.4.5 Moderating Variables	62
3.4.6 Reliability	62
3.4.7 Validity	63
3.5 Structural Model	64
3.6 Common Method Variance	64
3.7 Summary	65
4. Results	67
4.1 Introduction	67
4.2 Descriptive Statistics	68
4.3 Data Analysis	68
4.4 Measurement Model Analysis	70
4.4.1 PLS-SEM Model 1	70
4.4.2 Convergent Validity	71
4.4.3 Internal Consistency	72
4.4.4 Discriminant Validity Analysis	74
4.4.5 Zero-Order Correlation	77
4.4.6 Common Method Bias	78
4.5 Structural Model Analysis	79
4.5.1 Hypothesis Results	81

4.6 Post-Hoc Analysis	82
4.6.1 PLS-SEM Model 2 - Moderating Variables	85
4.6.2 Second Order Analysis of PLS-SEM Models	87
4.7 Summary	88
5. Conclusions, Implications, Recommendations, and Summary	89
5.1 Discussion	89
5.2 Implications	92
5.3 Limitations	93
5.4 Summary	96
References	119
Appendices	98
A. Data Collection – Online Survey Instrument	98
B. Permission for CCI-R+ Instrument	113
C. Company-Paid Approval to Conduct Research	115
D. Participation Letter	116
E. Survey Recruitment Cards	117
F. IRB Approval Letter	118

List of Tables

Tables

1. Criminal Behaviors and Definitions	35
2. Descriptive Characteristics of the Full Sample	68
3. Factor Loadings for Cyberstalking With 18 Indicators	71
4. Factor Loadings, Reliability, and Validity Statistics for Study Constructs	73
5. Heterotrait–Monotrait (HTMT) Results	76
6. Cyberstalking Indicator Cross-Loadings and Construct Correlations	76
7. Zero-Order Correlations Between Study Constructs	78
8. Harmon’s Single-Factor Test	78
9. Path Coefficients for PLS-SEM Model 1	80
10. Path Coefficients for PLS-SEM Model 2	86
11. Path Coefficients for Second Order PLS-SEM Models	88

List of Figures

Figures

1. Attribution Theory (Heider, 1958)	49
2. Psychosocial and Behavioral Attribution Model	50
3. Conceptual Model	51
4. Structural PLS-SEM Model 1	80
5. Concept of Structural PLS-SEM Model 2	82
6. Moderating Variable Assessment	84
7. Structural PLS-SEM Models 1 & 2 with Second-Order	87

Chapter 1

INTRODUCTION

1.1 Background

“Technology changes everything, crime included” (Clarke, 2004, p. 1). As technologies become more relevant to and engaging for targeted audiences, it is more probable that social networking sites (SNSs) will become a primary venue for cyber threats and cybercrime. Most crimes are a product of proximity, and SNSs provide a virtual proximity for deviance and cybercrime, ultimately resulting in cyber-victimization. SNSs such as Facebook have grown exponentially to over 1 billion active users, comprising 79% of Internet users,— including 68% of all U.S. adult Internet users (Pew Research Center, 2016). The potential range of victims is therefore quite large and broad.

SNSs are Internet-based services that allow individuals to:

- 1) Construct a public or semi-public profile within a restricted system,
- 2) Articulate a list of other users with whom they share a connection, and
- 3) View and navigate their list of connections and those made by others within the system (Boyd & Ellison, 2007).

Another prominent characteristic of social networks is the so-called small-world effect or the famous six degrees of separation (Travers & Morgan, 1969). The emergence of social networks has since clouded that theory. Backstrom et al. (2012) reported the first world-scale social-network graph-distance computations, using the entire Facebook network of active users. The authors determined the average distance between users is 4.74 intermediaries or degrees of separation. As Facebook has grown over the years, representing a larger fraction of the global population, it has

become progressively more connected. Researchers at Facebook (Edunov et al., 2016) have tapered the number to 3.5 degrees of separation. This close virtual proximity of users has made it easier to distribute threats within SNSs.

SNSs have provided a platform for an overabundance of threats to gain momentum over the years. Zheleva and Getoor (2009) revealed how an enemy can exploit an online social network with a combination of public and private user profiles to predict the private attributes of the users.

Intensified IS research is in demand for constructing a secure social networking platform, as it is critical in turning SNSs into successful collaboration tools. Traditional theorists of cybersecurity emphasize protecting against attacks from external threats (Nurse et al., 2014a). This study considers a less traditionally recognized threat: the insider threat within SNSs, that arising from within users' own networks. There have been exhaustive discourses on everything from what exactly an insider threat is (Hunker & Probst, 2011), and what the range of human and psychological factors involved are (Greitzer & Hohimer, 2011), to how threats can be predicted, identified, and effectively addressed with the rise of technological and behavioral advances and theories (Nurse et al., 2014b). A sociomaterial approach places attention on the practices of individuals taking situated actions and the consequences that those individuals and actions generate. The sociomateriality of online social networking is constituted by three categories of behavior based on the online social networking technology, online social networking tasks, and online social networking environment (Thambusamy & Nemati, 2011).

Additionally, Johnson et al. (2012) found that most users are concerned about the outside threat of strangers viewing their profiles, rather than the threat of inappropriately sharing content with members of their friend network. Although SNS global privacy settings have aided users in coping with the threat of outsiders viewing content, they do not adequately address the insider

threat. This can be of interest to various entities inside and outside of SNSs, which can expose SNS users to a plethora of threats (e.g., stranger vs. acquaintance crime), posing a problem among outside versus internal audiences within SNS circles.

While most SNSs encourage acceptable behavior and adherence to community standards (Facebook, 2016), incidences of information deception, disruption, and destruction are rampant. The FBI Internet Crime Complaint Center (IC3) reported more than 288,000 complaints related to cybercrimes in 2015 (FBI, 2016). These examples of unacceptable behaviors have been known to stem from certain personality traits. Because traits play a common role in human reasoning and behavior, it is reasonable to anticipate that personality plays a part in threat processes and outcomes. It is also necessary to articulate the major challenges for understanding threats in the context of SNSs, particularly from a personality and behavioral-specific perspective and emphasizing the specific motivations of individuals and their actions or intentions.

The proactive course for threat analysis is to take behavioral or psychosocial data into account to capitalize on signs and precursors of the malicious activity. It has been established that personality traits influence human behavior, but there is much to be understood about what motivates individuals to exude certain malevolent behaviors. One lens that can be used to examine these behaviors focuses through the “Dark Triad” personality traits. The Dark Triad refers to three interrelated higher-order personality constructs: narcissism (i.e., excessive self-love), Machiavellianism (i.e., manipulative attitudes), and psychopathy (i.e., lack of empathy) (Paulhus & Jones, 2011). While billions of users have adopted SNS technology, it is not currently known whether these users have any commonalities or represent a certain personality type. Several lines of research suggest that the Dark Triad may facilitate a social style geared towards exploiting others in social contexts (Jonason et al., 2009).

Buonanno (2003) asserts that there are various factors that “drive” people to carry out cybercrime; they are driven by the desire to fulfill or satisfy malevolent “needs,” then indulge in the act. Woodworth (1918) introduced the term “drive” into American psychology; distinctions have been made between the terms “needs” and “drives” or “motives.” There are different theories of human needs, but the most widespread, exploitable, and relevant to this research is Maslow’s theory of human motivation (Maslow, 1943). The needs outlined therein motivate both valid users and malefactors within social communities to perform certain actions. But understanding motivation is a complex undertaking, as there are various inter-related factors that may alter outcomes.

There are several motivation theories that examine characteristics of hedonic motivation and behavior and rely on such qualities to better understand human purpose and human nature. Attribution theory (Weiner, 1985), a hedonic motivation theory, is a good explanation for an event or behavior. Sledgianowski and Kulviwat (2009, p. 3) “consider SNSs within a hedonic context, primarily used to bring enjoyment and pleasure to their users.” In the context of SNS malevolent behaviors, attribution helps to identify and avoid the behaviors and factors that cause them to occur. Attribution theory suggests that attributions for these behaviors and outcomes ultimately help to form emotional and behavioral responses (Weiner, 1985).

Black, Woodworth, and Porter (2014) conducted one of the first research projects exploring whether Dark Triad individuals also will have an enhanced ability to detect susceptibility in individuals, as well as the verbal and non-verbal cues that they use to detect vulnerable people. There has been very little reported on how to evaluate a threat susceptibility algorithm, especially for SNSs. This study highlights that criminal behaviors should be examined in the context of changing technical, social, behavioral, and motivational factors. By examining certain behavioral

characteristics of threat actors, the likelihood of criminal disposition and another deviancy can be predetermined.

Research has been conducted regarding this debate, which has resulted in a conclusion that both personality and environment do play a role in the criminality of an individual. The definition of criminal behavior and its distinction from antisocial behavior could be the topic of considerable discussion. For simplicity's sake, the term *criminal* refers to behavior that is sanctioned by the legal system. A common denominator across many research studies is the fear that the Internet will generate a critical mass of deviants, which would foster justification for socially unacceptable forms of behavior, or encourage criminal behaviors (McDonald et al., 2009). Online deviant behavior refers to a variety of actions, some considered criminal or amoral, many considered both.

In research, it is important to explicate the relationship between digital technologies, their environments, and human behavior. Exploration of deviant and criminal behaviors through examination of what goes on inside the minds of SNS users has taken a back seat to Information Systems (IS) research. This research investigates whether individuals who commit deviant and criminal acts within SNSs display Dark Triad attributes; consequently, the psychosocial perspective of threat actors within SNSs should be examined. In this research, the *foci* of cyber threats are malicious, where the threat actor intends to cause harm within SNSs; as a result, accidental threats lie outside this study.

Determining what constitutes criminal behavior can cover a variety of actions and for that reason, researchers tend to focus on the wider context of antisocial behavior. Morley and Hall (2003), who investigated genetic influences on criminal behavior, argue that there are three different ways to define antisocial behavior:

1) Equating it with criminality and delinquency, which both involve engaging in criminal acts. Criminality can lead to arrest, conviction, or incarceration for adults, while delinquency is related to adolescents committing unlawful acts (Rhee & Waldman, 2002);

2) Equating it to diagnosis of certain personality disorders, such as Antisocial Personality Disorder, which is linked to an increased risk for criminal activity; 3) Equating it by examining personality traits that may be influential in the criminal behavior of individuals. Personality traits such as aggressiveness and impulsivity are two traits that have been frequently investigated (Morley & Hall, 2003).

It is important to understand the psychological mindset of individuals to integrate key insights about human behavior conjointly with technical solutions to develop mitigation techniques. Criminological research has expanded its focus over the last few years to address the various technology-enabled crimes and the applicability of extant theories to account for virtual malevolent behaviors (Taylor et al., 2014). Hence, it is necessary to conduct a systematic review of the literature, given the range of methodological and theoretical perspectives that have since been employed. Further details of personality traits associated with cyber-criminal behavior is discussed later in this paper.

1.2 Problem Statement

Information Systems offer many ways to share information, having an impact far beyond the world of business and organizations. As information systems become increasingly pervasive and personalized (Lyytinen & King, 2004), the use of SNSs and the behaviors related to their use will increase. This study is an empirical examination of whether individuals who negatively impact SNSs may possess Dark Triad personality attributes, exhibiting deviant or criminal behaviors, and ultimately leading to the outcome of criminal threats within SNSs.

Over the years, extensive psychological research has been conducted on personality traits and disorders. Recently, the vast majority of IS research involving personality traits has focused primarily on the Big Five traits: openness, conscientiousness, extraversion, agreeableness, and neuroticism. The Big Five Model of personality is a theory developed from both language taxonomy as well as statistical factor analysis (Costa & McCrae, 1992). In the last decade, personality psychologists have turned their attention to the dark side of human character: Machiavellianism, psychopathy, and narcissism. Collectively, these traits are widely known as the Dark Triad model (Paulhus & Williams, 2002). The Dark Triad is quickly growing to be a popular topic (Jonason et al., 2009; Paulhus & Williams, 2002), and its traits are associated with a value system of unconventional and antisocial morality (Kajonius et al., 2015).

Although several IS researchers have studied deviant behavior in the past, there is a lack of IS research tracing the Dark Triad personality traits within the context of SNSs and its accompanying deviant behaviors. Most SNSs are considered communal services and have specific communal policies of what conduct they will or will not allow from users of their service. More specifically, Facebook (2016) has community standards guidelines to provide clarity on the deviant behavior it allows or prohibits on its service. Ironically, SNSs are also used as a tool for deviant behaviors, such as nudity or pornography, racism or hate speech, violence or graphic content. Because deviant behaviors are not necessarily criminal in context, yet all criminal behavior stem from deviance, there is no clear individual or group that serves to regulate deviant behaviors on the Internet or SNSs. This study tries to recognize practitioners of deviant behavior based on their characteristics in correlation with the Dark Triad personality traits and impact in SNSs which can consequently morph into criminal behaviors.

Gove (1985) reviewed six of the most influential theories of deviance: labeling theory, conflict theory, differential association theory, control theory, anomie theory, and functional theory. Gove concluded, “All of these theoretical perspectives either explicitly or implicitly suggest that deviant behavior is an amplifying process that leads to further and more serious deviance” (p. 118).

Latour’s actor-network theory (ANT) provides a theoretical lens for conceptualizing and analyzing the human-technical relationship (Law & Hassard, 1999), which is becoming deep-rooted within the field of criminology (Brown, 2006). Criminological research has identified participation in deviant behaviors as a risk factor for a variety of types of victimization (Lauritsen et al., 1992), including cyber victimization (Bossler & Holt, 2009). One of the main challenges within the modern field of criminology is the increasing role of technology in crime and how to conceptualize areas of criminal activity where the nature of human-technical relationships is deeply intertwined (Wall, 2017; Brown, 2013:2006; Grabosky & Smith, 1998). Part of the challenge lies in the lack of theories of the techno-social to provide an adequate theoretical framework for the analysis of crime within criminal contexts where technology plays a strong role.

In the context of SNSs, there is a need to investigate the different effects of Dark Triad traits and criminal behaviors exerted by threat actors within SNSs. According to Larsen and Buss (2010), personality has consequences for the manner in which individuals act, how they view themselves and the world, their personal feelings, and how they react to certain circumstances. In addition, personality traits influence how individuals interact with others (Larsen & Buss, 2010), particularly within SNSs. Hence, a thorough understanding of why people behave the way they do naturally requires personality, social psychology, and criminology to be cognizant of one another. It is critical to understand one’s personality and the illicit actions related to such in the digital space

of SNSs. To understand the criminal behavior of SNS threat actors, it is necessary to examine the traditional psychological theories of criminal behavior and how they may be applied to develop a definitive understanding of a cybercriminal threat.

1.3 Dissertation Goal

The overall aim is to advance the field of IS research by producing through causal modeling a psychosocial behavioral model that can aid researchers and IS practitioners in determining precursors to predict threats within SNSs. There is a need to examine attributing psychological factors of criminal behaviors and their relationships that reveal threat actors or trust-betrayers within SNSs. This would allow users to contemplate more clearly personality and behaviors within them.

The effects and implications of human behavior should be a major consideration of any such effort, to the extent that all actors within SNSs need to be educated about cyber threats and their consequences. Implications can also be drawn regarding the maintenance of online interpersonal relationships. An examination of how dispositional attributions of personality traits causes or relates to criminal behavior would be a meaningful extension to this area of research. Understanding the motivational underpinnings of dark traits may inform the understanding of emotional and behavioral reactions. Therefore, there is a need for adequate theoretical lenses to help explain the complex interplay of human-technological relationships involved in cybercriminal activity within SNSs. The practical implications of this study are in raising awareness and stimulating the thinking of social media outlets, law enforcement, and SNS users around the potential criminal effects behind the Dark Triad and cybercriminal behaviors.

1.4 Research Question

This study presents a model that aims toward understanding criminal behaviors based on personality traits. It uses psychological and behavioral profiling to identify potentially dangerous users. The model consists of three anti-social constructs (i.e., the Dark Triad) that represent personality at the highest level of abstraction that proponents of the model believe can classify differences in the personalities of individuals. These constructs summarize more specific facets, which are themselves made up of individual traits (Gosling et al., 2003). The uniqueness of the model is that it is an interdisciplinary approach, in the sense that it combines criminal outcomes with approaches that draw upon psychology and human behavior. Threat actors continue to innovate, using top cyber threats and new deception techniques to infiltrate SNSs and cause damage to unsuspecting or susceptible users. The behaviors of threat actors may point toward a common psychological stance that can offer possibilities for interdicting their criminal SNS actions. Therefore, the following fundamental research question is important to address as follows:

RQ1. Is there a relationship between the Dark Triad characteristics and cyber-criminal behaviors on social networking sites?

1.5 Importance and Relevance of Research

SNSs have gained minimal attention from IS researchers and grown steadily as a topic of research. Between 2004 and 2013, 136 articles were published related to SNSs in the top ten IS journals (Cao et al., 2015). The accumulated research has not appeared to examine new and pressing issues in social networks; available knowledge needs to be synthesized and research gaps need to be addressed (Bandara et al., 2011). Hu et al. (2011, p. 447) describe SNSs as a “social hedonic-oriented type of IS, primarily used in a non-work environment” helping “users attain a sense of hedonic fulfillment in achieving personal needs” (Hu et al., 2011, p. 444). SNSs should

be represented more within the IS body of knowledge. Outside of a few studies related to cyberbullying (Dempsey et al., 2010) and cyber harassment (Melander, 2010), however, little IS research has been done specifically on the subject of deviant behavior as it relates to SNSs, whereas the majority of the research performed has come from the field of psychology. The primary aim is to establish and test; there are no current plans to apply the model to different sociodemographic groups or to wider regions or national populations. The significance of this study may also be viewed in terms of the contribution of the findings to both IS theory and practice.

Further, the Dark Triad has not been sufficiently studied in the IS literature on deviant or criminal behaviors on SNSs. Therefore, as a potential for original work, a combination of a suitable taxonomy and model can form the basis of a language for detecting and predicting SNS threat actors. This study's relevance is to provide a way for users to discern potential threats and a sense of susceptibility within SNSs. One way to capture the essence of SNS cybercrime is to examine the personalities and behaviors as they occur in the real world and to apply the results thereof to the virtual.

It has been previously argued that personalities are what determines human behavior. Jessor and Jessor (1977) built a social-psychological theory of "problem behavior" (deviance) which incorporates Rotter's (1954) learning theory and other personality and social variables. Their theory consists of three categories of variables: personality, social, and behavioral. The Dark Triad personality traits (i.e., narcissism, Machiavellism, and psychopathy) encompass these three categories and, according to research, have been known to lead to deviance – including criminal behaviors.

As identified earlier, narcissism forms one of the three personality constructs of the Dark Triad model. The narcissistic personality is marked by grandiosity, a sense of entitlement, and a

lack of empathy (Smith & Lilienfeld, 2013). O’Boyle et al. (2012) agreed with this description, adding that extreme self-aggrandizement is the hallmark of narcissism, which includes an inflated view of self; fantasies of control, success, and admiration; and a desire to have this self-love reinforced by others. Machiavellianism (MACH) refers to interpersonal strategies that advocate self-interest, deception, and manipulation. Deception plays an important role, as individuals must be aware of the masquerades they and others portray in SNSs.

Previous research, not explicitly concerned with psychopathy, has examined the relation between computer crime and specific personality traits. The research suggests cyber criminals score high on exploitive manipulative amoral dishonesty. Literature has gradually emerged examining “psychopathy-like” traits in the general population (Board & Fritzon, 2005; Ross et al., 2004). High cognitive and low affective empathy may depict individuals with antisocial behavior who are withdrawn and more impulsive (Jolliffe & Farrington, 2006). These “psychopathic-like” personality traits have been studied in relation to aggression and are grouped into three dimensions, *interpersonal* (e.g., grandiosity, egocentricity), *affective* (e.g., remorselessness, callousness), and *behavioral* (e.g., impulsiveness, irresponsibility). Notably, of all individuals with personality disorders, psychopaths are the most studied in psychology and psychiatry (Boddy et al., 2010).

The blatant disregard for personal privacy and information sharing within SNSs has, in some cases, proven to be detrimental. SNS users deliberately give out as much information as possible for adding friends or becoming popular (Acquisti & Gross, 2006). Yet many people spend an unprecedented amount of time interacting with SNSs and uploading large amounts of personal information. Cyber criminals may use this to their advantage and use fake identities to obtain user private information on SNSs. As a result, a lot of personal data is deliberately leaked into the public domain by the users and their audience (e.g., friends). This data can be of interest to various entities

inside and outside of the SNS, which exposes the SNS users to various kinds of threats (Kumari, 2010).

Lastly, this study is in the province of quantitative research methods. The aim of the quantitative research method is to test predetermined hypotheses and produce generalizable results (Marshall, 1996). Using statistical methods, the results of quantitative analysis can confirm or refute hypotheses about the impact of the affected participants. The lack of validated and reliable psychometric instruments for research in non-traditional criminal behavior (i.e., cybercrime) is a corollary problem with there being a lack of empirical research by the behavioral sciences in the area of criminal/deviant computer behavior. This study sought to spark a conversation about promising solutions to some of the current problems and potential approaches of how to create standards for future research in the new area of cyber-criminology. Future work in this area will profit from advances in SNS and personality-related methods overall.

1.6 Barriers and Issues

The attachment of the label "deviant or criminal behavior" is often dependent on the personal demographic characteristics of the offenders themselves. Demographics such as age, sex, ethnicity, region, and religion can all play an important part in assessing whether or not a particular behavior is to be treated as deviant or criminal. Prior research (Vassalou et al., 2010) shows that there might be cultural differences in people's behavior on Facebook. Especially with regard to disclosure, culture and religious upbringing might have a significant impact, not only on behavior but also on the amount of threat associated with the behavior. Other research identified different types of people who use Facebook (Barker, 2009) and found that the specific gratifications of Facebook use differ as a function of individuals' personality traits (Ross et al., 2009). This same evidence can be seen in other social media outlets across the globe.

Due to the secrecy often involved in criminal or deviant behavior, individuals typically are unwilling to report their actual behavior and actions. Analyzing any intentionally illicit community poses difficulties for the researcher. The global and anonymous nature of computer-mediated communication exacerbates such problems, because generating a research population from the hacker community necessitates self-selection by subjects and it was difficult to check the credentials of each subject.

The hacking culture is male dominant with an associated misogyny. Literature on hackers has failed to uncover any significant evidence of female hackers (Taylor, 1993). Having a personality predisposition for criminal behavior and the right environment can increase the probability of criminal activity. The nature of the potential computer deviant subjects may make it difficult to develop a sampling frame. Jones (2005) took criminal behavior further to describe actions relating to antisocial behavior. This identification of an antisocial personality with criminal behavior leads to the idea that criminal mischief is more prevalent in males. While our justice system is heavily loaded with male criminals, women are still part of the criminal “world.”

Research for this study and literature on hackers may not uncover any significant evidence of female hackers (Turtle, 2005:1984). This imbalance is disproportionate even in the field of computer-mediated technologies (Spertus, 1991). A number of factors explain the paucity of women generally in the computer sciences: childhood socialization, where boys are taught to relate to technology more easily than girls; education in computers occurs in a masculine environment; and a gender bias toward men in the language used in computer science (Spertus, 1991; Turtle, 2005).

There are two types of validity: internal and external. Regression, selection, and experimenter expectancy are threats to external validity. Threats to external validity are evaluated

by tests of the extent to which one can generalize across various kinds of people, settings, and times – in essence, tests of statistical interactions (Cook & Campbell, 1979). The largest internal validity threat in this particular research study is whether the instrument is viable and measures a true susceptible technique. External validity threats for this study are dependent on the response rate from participants.

1.7 Assumptions, Limitations, and Delimitations

One of the significances of reporting limitations is that it allows a researcher to be self-aware and minimize the severity of limitations in the design and in the conduct of a study (Baron, 2008). Assumptions, limitations, and delimitations can cause a study to be less reliable. By acknowledging the assumptions, limitations, and delimitations, the researcher performs a risk assessment and evaluates the impact of the research (Berner & Flage, 2016).

1.7.1 Assumptions

An assumption is “a statement that is presumed to be true, often temporarily or for specific purpose ... the condition under which statistical techniques yield valid results” (Vogt & Johnson, 2011, p. 22). It is important to emphasize the intertwined nature of the assumption about objectivity and the assumption that a reality exists external of the researcher. Leedy and Ormrod (2010) posited, “Assumptions are so basic that, without them, the research problem itself could not exist” (p. 62). It is impossible to achieve complete objectivity but cultivating an awareness of potential threats and taking measures to decrease threats whenever possible serves to strengthen the research study. Hence, this study presents the following assumptions:

- 1) It is assumed that the sample subjects would complete the survey without response bias.
- 2) It is assumed that survey participants can take the survey from any compatible smart device.

- 3) It is assumed participants are recruited from the general community, and not from criminal or psychiatric settings.
- 4) It is assumed that the survey respondents or sample subjects have the fiscal, mental, and physical capacity to complete the survey.
- 5) It is assumed data collection instruments are valid and reliable based upon prior research and their prior use.
- 6) It is assumed that the analytical software, including those for confirmatory factor analysis (CFA) and structural equation modeling (SEM) analyses – is accurate in measuring the data.

1.7.2 Limitations

Limitations are potential weaknesses in the study beyond the control of the researcher (Leedy, 2010). The objective in this section is to recognize the potential, integral, and salient limitations that could threaten the results or the internal validity of this study. Therefore, issues associated with sampling method, data collection methods (Sekaran & Bougie, 2016), low response rate, lack, completion rate, and possible response bias or lack of candor (Baron, 2008) are some of the limitations that may be identified in this study.

1) *Sampling method.* The proposal in this study is to use convenience sampling. Convenience sampling involves the collection of data from a convenient and available sample subjects in a given population (Sekaran & Bougie, 2016). An adequate sample size is necessary to perform all this study's statistical analyses. PLS path modeling parameter estimates are biased, with the bias diminishing as both the number of indicators per construct and sample size increase. Researchers can calculate the expected degree of bias and determine the likely impact of investing in a larger sample size (Dijkstra, 2010; McDonald, 1996).

2) *Data collection*. The data for this study was collected via a website, and the link for the web address or the universal resource locator (URL) was sent to the participants via email, social media, and text messages. There is a potential for response bias, which could threaten internal consistency, and a researcher has no control over the response time (Sekaran & Bougie, 2016).

Although there is considerable empirical support for the validity of personality self-report measures (Jones & Paulhus, 2014; Paulhus & Williams, 2002), many studies benefit from the use of informant-report personality measures or scenario-based surveys to alleviate dishonest responses. Perhaps the most important feature of informant reports is that, unlike self-reports, they can be aggregated across observers to obtain a more reliable assessment of personality (Block, 1961; Hofstee, 1994). Cronbach's *alpha* for any reliability test will likely be reduced if respondents have limited literacy or intelligence (Allik et al., 2004), if they are responding in a second language in which they are not fully fluent, or if they are uncooperative and respond randomly.

3) *Dark Triad Analysis*. Some researchers have argued that the level of assessment should dictate whether the traits should be combined or separated (Jonason et al., 2011), but SEM approaches to the Dark Triad statistical approach are also flawed. Though SEM allows shared variance to be assessed and utilized, spurious relationships among lower level variables can lead to statistical illusions that higher order factors exist, when in fact, no such shared variance does (Ashton et al., 2009). As such, PLS-SEM suffers from the limitation that there may be an overestimation of shared variance among the Dark Triad traits. Last, there is ample evidence that suggests that men score higher on all three of these traits than women (Jonason, Li, & Buss, 2010; Jonason et al., 2009) and therefore men should score higher than women do on the Dirty Dozen measures.

1.7.3 Delimitations

Delimitations are self-imposed (Creswell, 2017) or established boundaries or parameters by a researcher to understand the constraints of the research and manage a study better. Typically, it describes the scope of a study in terms of its sample size, data collection demographic and geographical reach, survey instrument design, and the like (Baron, 2008). Therefore, the primary delimitations pertained to the design of this study and provided boundaries for the research.

- 1) Responses are self-reported by participants.
- 2) The respondents are bounded by time to voluntarily complete the survey.
- 3) The beliefs of the participants at the time they answer the survey.
- 4) The sample size envisioned for this study is a minimum of 200 subjects based on the review of existing and prior literature. There may be no allowable scope for recruitment of an equal gender ratio of participants.
- 5) Participants are anyone who is 18 years of age or older. In addition, the geographical reach includes anyone within the continental United States and those outside but in a U.S. territory or jurisdiction.

1.8 Definition of Key Terms

Definitions of key terms used throughout this document are provided below to offer explanation on the constructs and methodology of this study:

- 1) *Dark Triad* - Refers to three interrelated higher-order personality constructs: narcissism (i.e., excessive self-love), Machiavellianism (i.e., a manipulative attitude), and psychopathy (i.e., lack of empathy) (Jones and Paulhus, 2014). The Dark Triad embodies the most prominent, socially aversive personalities characterized by a common underlying deficit in empathy.

2) *Dirty Dozen Dark Triad (DTDD)* - Large- scale studies in which multiple personality traits are assessed are a lengthy assessment procedure and not practical. Aiming to solve this problem, Jonason and Webster (2010) developed a concise questionnaire to assess the Dark Triad traits, the Dirty Dozen scale. The scale consists of 12 items, four for each of the three traits comprising the Dark Triad.

3) *Cybercrime* - The use of computers and the Internet by criminals to perpetuate fraud and other crimes against companies and consumers (Chaubey, 2009, p. 135).

4) *Cyberstalking* - A group of behaviors in which an individual, group of individuals, or organization uses information technology to harass one or more individuals. Such behaviors may include, but are not limited to, the transmission of threats and false accusations, identity theft, data theft, damage to data or equipment, and computer monitoring per Bocij & McFarlane (2002). In cyberstalking, perpetrators do not have to engage in direct contact with the victim.

5) *Cyberbullying* - Cyberbullying is an umbrella term related to similar constructs such as online bullying, electronic bullying, and Internet harassment. Dehue et al. (2008) suggest that three necessary conditions must be met for a situation to be considered cyberbullying: the behaviors must be repeated, involve psychological torment, and be executed with malevolent intent.

6) *Unethical Hacking* – When skilled individuals use their abilities illegally to harm society by finding vulnerabilities in computer systems and attacking them, creating and distributing virus-containing programs for personal gain. This is considered unethical and criminal, which is prosecuted in accordance to U.S. laws (Sukhai, 2004).

7) *White Hat Hacker* - An individual legal hacker who provides security to cyberspace. The ethical or proactive approach to locate security vulnerabilities in companies or organizations before the

unethical hackers do. The proactive approach is sometimes called “*ethical hacking*” (Labuschagne, 2004).

8) *Black Hat Hacker* - A hacker is one who illegally breaks into a network system to steal information or money, and sometimes to cause damage by inserting viruses, malware, or other malicious software. A hacker in the sense of unethical hacking is a black hat hacker.

9) *Identity Theft* – A rampant form of cybercrime, which is usually described as stealing an individual’s identity by illegally accessing unique identifiers such as passwords, digital signatures, and other personal identifiable information (PII) with the intention to perpetrate a crime using computers and other communication devices over the Internet (*idtheftcenter.org*).

10) *Attribution Theory* – A hedonic motivation theory developed by Fritz Heider (1958), which suggests that we tend to give causal explanations for someone’s behavior, often by crediting either the situation (behaviors) or the person’s disposition (personality).

1.9 Summary

This study is presented in three chapters. Chapter One, the introduction, included the background and context of the study. In addition, the statement of the problem, purpose of the study, research questions, significance of the study, conceptual framework, and terminology of the study are identified. In addition, the barriers and issues of the research followed the aforementioned, including the assumptions, limitations, and delimitations. Chapter Two is a thorough review of relevant literature on the Dark Triad personality traits, cybercrime, and criminal behaviors, including the theoretical framing, conceptual model, and hypotheses. Chapter Three details the methodology used to conduct the study, research design, survey instruments, plans for data collection and analysis.

Chapter Four discusses the results of the data analysis. Chapter Five presents and the discussions, findings and implications. Throughout this study, the relevant justification for the research methods used and the design of the model based on established research is provided. A review of the literature of related areas of research is presented in the next Chapter.

Chapter 2

LITERATURE REVIEW

2.1 Introduction

This chapter reviews the theoretical groundwork and empirical findings regarding personality and crime. This study investigates personalities and criminal behaviors contributing to cyber threats, vulnerabilities, and risks that endanger the privacy of SNSs and their users. Though SNSs have many positive features, there are some drawbacks that potentially can be misused with criminal intent and/or for destructive goals. Somewhat inherently to their nature, SNSs provide an environment in which cybercriminals can propagate malicious software, cyberstalk, cyber bully, commit identity theft, and launch hacking attacks against victims' computers.

Currently, SNSs are facing myriad threats. To eliminate or at least understand SNS threats, it is important to examine the personalities and behaviors behind the cybercriminals responsible for these threats. This section reviews the state of the art of cyber threats to current SNSs, mainly focusing on psychological and criminal behaviors. Understanding how this study unfolds, requires some background in psychological constructs.

A substantial amount of research is examined to discern the following: a) how the construct of personality has developed over time in the field of psychology; b) psychology and criminology theory, discourse, and research; c) what inferences can be drawn from the current crime and personality literature; d) how personality fits into current theories such as attribution theory and evolving criminology; and e) whether personality can be used to predict criminal behavior. An examination of relevant research appears below.

2.2 “The Dark Triad”

The word “personality” comes from the Latin word *persona*, which refers to the disguise used by actors in a theater. This idea was derived from the understanding of personality as the combination of individualities or qualities that someone possesses. The first formal study of personality occurred within psychoanalysis, developed by Sigmund Freud (1923). Psychoanalysis takes a relatively dark view of human nature; Freud (1923) argued that the mind could be divided into three abstract categories or structures. These are the id, the ego, and the superego, all developing at different stages in our lives. The id (impulsive and unconscious) is the biological component of personality; ego is “that part of the id which has been modified by the direct influence of the external world” (Freud, 1923, p. 25), the rational component of the personality that acts according to the reality principle; and “superego” corresponds to the moral side of the personality, being composed of consciousness (Hall et al., 2000). More recently, Mairesse and Walker (2006) have contended that personality can be defined as a set of attributes that characterize an individual and involves behavior, temperament, emotions, and the mind.

One of the major theoretical areas in this study of personality is the trait approach. The trait theory suggests that individual personalities are composed of broad temperaments. Allport and Odbert (1936) categorized personality traits into three levels: “Cardinal traits” are traits that dominate an individual’s whole life, often to the point that the person becomes known specifically for them. People with such personalities sometimes have their name become synonymous with these qualities, such as Freudian, Machiavellian, narcissistic, etc. “Central traits” are characteristics that form the basic foundations of personality (e.g., intelligent, honest, shy, and anxious). And “secondary traits” are traits that are sometimes related to attitudes or preferences and often appear only in certain situations or under specific circumstances.

Over time, there has been increased interest in better understanding the relationship between personality traits and the use of information systems (Hamburger & Ben-Artzi, 2001). Extant research suggests that personality variables act as antecedents to attitudes, cognitive behaviors, and *a priori* involvement with information technology (Zmud, 1979). As evidenced by research (Junglas et al., 2008), there are three reasons to focus on personality constructs:

- 1) Personality variables are recognized to be important in the decision-making and IS literature as they add to our knowledge about people's information processing styles, attitudes, and behaviors (Hair et al., 2014);
- 2) Information technologies become more personalized (Ackerman, 2004), and personality variables can influence how users perceive these and other technologies in security (Gonzalez & Sawicka, 2002);
- 3) Perhaps most importantly, personality traits can account for the influence of individual differences in determining the power of the attitudinal constructs (Junglas et al., 2008).

A growing body of IS research has pointed to the five-factor model (FFM) as a recurring and more or less comprehensive taxonomy of personality traits (McCrae & John, 1992), integrating the FFM into existing IS models and theories. The FFM traits consist of five constructs of personality that span across major personality inventories and research contexts. These include extraversion, agreeableness, conscientiousness, neuroticism, and openness to experience (Judge & Bono, 2000). Several IS studies have used aspects of the Big Five personality traits in studying the acceptance of the Internet, personal computers in the workplace, deviant workplace behaviors, and information privacy (Belanger & Crossler, 2011).

For example, Wald, Khoshgoftaar, and Sumner (2012) applied machine-learning algorithms to predict users' personality traits based on the FFM, using demographic and text-based

elements extracted from Facebook profiles. The authors extracted a set of attributes such as age, gender, location, and relationship status, as well as the number of friends, photos, interests, and comments provided to define each individual. Per the authors, the final results have privacy implications as they permit advertisers to focus on a specific subgroup of individuals based on their personality traits.

Though widely used in IS research, the FFM has faced criticism for failing to completely account for all individual differences in personality-related human behavior, specifically traits reflecting antisocial behavior (Veselka et al., 2012). Subsequently, attention has been brought to the darker antisocial behaviors within the Dark Triad personality traits (Paulhus & Jones, 2011). The DT embodies the most prominent, socially aversive personalities, characterized by a common underlying deficit in empathy (Reid, 1995). The DT personality traits encompass three conceptually distinct, but empirically overlapping constructs: narcissism, Machiavellianism, and psychopathy (Paulhus & Jones).

There are at least two ways that a personality characteristic can be called “dark” – in its nature or in its effects. We can claim that a personality concept is dark if it has a particularly malevolent character; individuals who have high elevations on the construct are motivated (consciously or unconsciously) to harm others (or themselves). On the other hand, a characteristic that has no particularly malevolent content could still have noxious consequences. Harm, of some kind, is almost a necessary consequence of the label dark – (Spain et al., 2014, p. 10).

Narcissism, which has been widely studied as a personality disorder (APA, 2013), has been conceptualized as a “normal” personality variable characterized by dominance, exhibitionism, and exploitation, along with feelings of superiority and entitlement (Raskin & Terry, 1988). Individuals displaying narcissistic personalities have an inflated self-absorption and focus largely on themselves (Emmons, 1984). One consistent finding in the narcissism literature is that narcissists

see themselves as being intelligent, extroverted, and open to experience, but not necessarily as moral or agreeable (Campbell et al., 2002). When confronted with an ego threat, narcissists have been found to react with aggressive behavior, at least in controlled experimental settings (Jones & Paulhus, 2010; Twenge & Campbell, 2003). Machiavellianism refers to individual differences in manipulativeness, insincerity, and callousness (Christie & Geis, 1970), and has been widely studied in social psychological investigations involving persuasion, leadership, and ethical behaviors.

According to prior researchers (Christie & Geis, 1970), people who score high on this trait are cynical, unprincipled, believe in interpersonal manipulation as the key for life success, and behave accordingly (Grimmelmann, 2010). Psychopathic behavior, as defined by the Diagnostic and Statistical Manual of Mental Disorders (DSM-V), is a personality disorder and an important psychological construct (APA, 2013). The transition from the DSM-IV to the DSM-V represents a potential breakthrough in the understanding of the nature of dark personality (Krueger et al., 2011a; Krueger et al., 2011b). The DSM-V uses a categorical classification approach, which has the advantage of simplicity and ease of communication (Widiger, 1992). Categorical classification of psychopathology, however, is extremely challenging; a psychological diagnosis is seldom defined by the presence of a single characteristic. Three significant qualities that characterize psychopathy include an arrogant and deceitful interpersonal style, deficient affective experience, and impulsive and irresponsible behavior (Jakobwitz & Egan, 2006), often exhibiting affective shallowness, lack of empathy and remorse, superficial charm, and manipulation (Hare, 2003). Foulkes et al. (2014) suggest that individuals high in psychopathy may be motivated by negative social potency in their interpersonal interactions. Although individuals high in psychopathy initially come across as normal and pleasant persons with high abilities, they demonstrate

irresponsible and unreliable behavior (Cleckley, 2016). Specifically, individuals high in psychopathy take pleasure in treating others cruelly (Foulkes et al., 2014).

The three DT traits are moderately inter-correlated, and each contains a degree of self-aggrandizement, aggression, and duplicity (Paulhus & Williams, 2002). Not many studies have examined all three DT traits at once (Paulhus, 2001), so most evidence for the positioning of the DT comes from studies using only one trait. Many researchers contend that the three traits may be best viewed as one's social orientation toward conspecifics.

Research shows that certain personality traits are correlated with the propensity of users to use social media and SNSs (Zhong, 2011). A more recent study that examined psychopathy and social media usage was the first study to examine machine prediction of all three DT personality traits using social media (Boochever, 2012). Boochever found that machine learning provides useful prediction rates, but is imperfect in predicting an individual's DT traits from Twitter activity. Consequently, Sumner et al. (2012) used linguistic inquiry and word count (LIWC) in a study to analyze and predict DT personality traits of Twitter users and examine whether machine learning could be used to predict these constructs based solely on Twitter usage.

Numerous studies have predicted the personality traits of users by analyzing their personal user behavior on SNSs (Kosinski et al., 2014; Sumner et al., 2012). For example, Ross et al. (2009) pioneered the study of the relation between personality and patterns of SNS use. The authors hypothesized many relationships between personality and Facebook features. While billions of users have adopted SNS technology, it is not currently known whether these users have any commonalities other than that use, or if they represent a certain personality type. Specifically, however, several lines of research suggest that the DT may facilitate a social style geared toward exploiting others in social contexts.

Current IS research (Maasberg et al., 2015) examined insider threat incidents with malicious intent and proposed an explanation through a relationship between DT personality traits and insider threats. The proactive course for insider threat analysis is to take “behavioral” or psychosocial data into account to capitalize on signs and precursors of the malicious activity (Greitzer & Frincke, 2010). A theory that SNSs breed narcissism has produced research with varied results, taking an important step in examining the SNS behaviors and motives of narcissists (Bergman et al., 2011). Additionally, research work has connected excessive usage of social media to the personality trait of narcissism (Buffardi & Campbell, 2008). In addition, there are claims that SNSs like Facebook and Twitter promote narcissism. Narcissistic components such as exploitativeness are considered destructive, relating with traits considered to be negative such as Machiavellianism (McHoskey, 1995). Machiavellian behaviors on SNSs are controversial in some respects. For instance, there are conflicting findings in terms of time spent on SNSs (Fox & Rooney, 2015; Garcia & Sikström, 2014).

It has been found that high levels of Machiavellianism predicted uses of both honest and dishonest self-glorification (Abell & Brewer, 2014). Machiavellianism has been theoretically (McHoskey et al., 1998) and empirically (McHoskey, 1995) linked to a subclinical form of psychopathy. In some psychological contexts, an exploitive tendency is a component or trait of a narcissistic personality (Millon & Grossman, 2007); however, the literature considers exploitation a reflection of an exploitative motive based on the propensity to strive for an advantage at someone else’s expense. More recently, Ahn et al. (2015) suggest narcissism as an important psychological factor that predicts one’s behavioral intention to control information privacy on SNSs. Literature has suggested that the DT traits have surfaced in major threats to SNSs.

2.3 Cyber Crime

Cybercrime is the use of computers and the Internet by criminals to perpetuate fraud and other crimes against companies and consumers (Chaubey, 2009, p. 135). Any criminal activity that uses a computer as an instrumentality, as a target, or as a means for perpetuating further crimes comes within the ambit of cybercrime. At the basic level of examination, there is no discernible control mechanism in place so far as terminology is concerned. Thus, one might speak of “cybercrime,” “computer crime,” or “digital crime” and be discussing the same concepts. A generalized definition of cybercrime may be “unlawful acts wherein the computer is either a tool or target or both” (Chaubey, 2009, p. 141). The definition of cybercrime and the differentiation of types of cybercrime are extremely important. Definitions provide researchers with a common language, necessary for sound collaboration (or meaningful argument). The approach to understanding cybercrime and efforts to home in on cybercriminal activity through efforts like digital forensics are changing from the more traditional (i.e., a technology focus) to one where society realizes the need to understand *the people* involved and their motives, basically the *who* and *why* of cybercrime (Crossler et al., 2013).

Cybercrime by its very nature crosses the digital divide. The Internet simply does not recognise international boundaries, nor do cybercriminals. Cybercrime and those individuals who engage in this deviant behavior have become a part of our digital society (Furnell, 2003). These crimes are not limited to domestic hackers but are increasingly emanating from other countries. Perhaps most serious and disturbing is the risk of overseas cyber-attacks being used to undermine key elements of the national infrastructure or the economy of a country. Given the widespread growth of the Internet and networking technologies within the global economy and social life, efforts to detect and eliminate cybercrime represent a serious challenge for law-enforcement

agencies around the world. Over the past decade, police and federal agencies have been challenged to respond to the increase in online cyber-attacks by setting up cybercrime units on the local, national, and international levels.

One of the challenges lies in the scarcity of techno-social theories to provide an adequate theoretical framework for the analysis of cybercrime within criminal contexts where technology plays a strong role. This would establish criteria for analyzing cybercrimes and criminals in the clear, unambiguous context of the virtual world. Another challenge in dealing with cybercrime is that we live at a time when computing is at the core of the knowledge economy and social life itself (Luppigini, 2009). The third challenge concerns the lack of knowledge about the myriad of cybercrime varieties that exist and continue to arise, including: cyber terrorism (Minei & Matusitz, 2011; Rid, 2012), cyber espionage (Lin & Luppigini, 2011), cyber stalking and online harassment (Madge, 2007), and cyberbullying (Goodboy & Martin, 2015).

The beginning of SNSs introduced connecting with people and building networks of healthy relationships in society. But it now offers cybercriminals a boundless gateway to target victims. The secure feeling of anonymity in SNSs encourages a person to commit cybercrimes that a normal person would not commit in the real world. Cybercrimes on SNSs include posting objectionable content on a user's profile, creating a fake profile to defame a person, and gaining access to someone's profile by unethical hacking. Zheleva and Getoor (2009) revealed how a threat actor can exploit an online social network with a combination of public and private user profiles to predict the private attributes of the users. Expectedly, there have been countless reports of cyber criminals "phishing" for personal information on SNSs. Magklaras et al. (2001) introduced a threat-evaluation system based on certain profiles of user behavior. Other approaches highlight the need for both technical and psychological approaches (Belanger & Crossler, 2011). Narayanan and

Shmatikov (2008, 2009) demonstrated how users' privacy can be weakened if an attacker knows of the presence of acquaintances among users within SNSs. There is also the possibility that specific personality characteristics are linked to specific attacks rather than all attacks. Finding them becomes more important, therefore.

Given the strong theoretical and empirical overlap between psychopathy and criminal behavior (Hare, 1996), psychopathy is emerging as an important construct in criminology (Polaschek & Daly, 2013). DeLisi (2016) argued that psychopathy should be considered the unified theory of crime because of its embodiment of the "pejorative essence of antisocial behavior" as well as its ability to accommodate both dimensional and categorical conceptualizations of antisocial behavior across diverse populations. Criminologists initially avoided the concept of psychopathy (and personality traits in general), even though psychopathy overlapped to some degree with other constructs within criminology.

According to Hare (1996), psychopaths are only concerned with looking after themselves and have no concern for the effects that their actions may have on others. They are completely unsympathetic to the suffering or the rights of others. Psychopaths have been related to several threats within SNSs, with online manifestation of psychopathy sometimes referred to as cyber-psychopathy. Nevin (2015) demonstrates that primary cyber-psychopathy is positively correlated with one's level of acceptance of deviant online behaviors, while both primary and secondary cyber-psychopathy are positively associated with one's tendency toward engaging in such misbehaviors. Their study would highlight the potential impacts of heightened psychopathic personality online. This exploration of the DT traits treats them as key constructs contributing to the role played by threat actors that has resulted in a generation of failure and erosion of SNSs.

2.4 Criminal Behaviors

Criminal behavior has always been a focus for psychologists, often revolving around the age-old debate between nature and nurture (Elsea, 1995). Research on the topic has resulted in a conclusion that both personality traits and environment play a role in the criminality of an individual. As new forms of technology emerge, they are exploited through new forms of criminal or deviant behavior (Thomas & Loader, 2000; Smith, 1998). Research scholars of deviant behavior and other fields have argued the possible causes of deviant behavior. The earliest studies of deviant behavior saw deviance as caused by pagan demonic possession or physical or biological physiognomies. Over the years, deviant behavior has been defined in various contexts. In a more summarized form, deviant behavior can be defined as the objective or subjective assessment of problem-producing behavior committed by an individual or group that affects the enjoyment of life or essential role of oneself or others (Gibbs, 2014).

The Internet presents some unique opportunities for deviant behavior (Rogers et al., 2006b, p. 246). SNSs also have been a factor in shaping a set of deviant behaviors, radicalization, and a range of other unacceptable behaviors (Kierkegaard, 2008). Recent studies investigating such phenomena have used Facebook more than Twitter because of the wider diversity of information that it has on user behaviors (Bachrach et al., 2012; Kosinski et al., 2014).

Human-based threats seem to be more attractive to researchers in the IS field, perhaps because of the complexity of understanding and predicting the human behaviors that lead to human vulnerabilities. When a person violates a social norm, it is considered to be a socially deviant action. A social norm can be defined as a “stable, shared conception of the behavior appropriate or inappropriate to a given social context that dictates expectancies of others’ behavior” (McKirnan, 1980).

Social media and information behavior research have frequently employed the FFM to predict human behaviors (Heinström, 2003, 2010). Yet, given that those high on DT traits manipulate others using coercive tactics (Jonason & Webster, 2012), the DT model has proven to be better at predicting deviant behaviors and examining their role in social media environments. The DT has gained much scientific consideration. Among various outcome measures, for instance workplace behavior (O’Boyle et al., 2012) or mating stratagems (Jonason et al., 2009), unethical or deviant behavior has been related to the dark traits: Psychopathy and Machiavellianism predicted exam-copying and plagiarism, respectively (Nathanson et al., 2006; Williams et al., 2010). Baughman et al. (2014) found that the DT, particularly Machiavellianism and psychopathy, was associated with lying in an academic context, but also with dishonesty toward mates.

Antisocial or criminal behavior appears to be a serious and pervasive problem in a variety of online social settings. SNSs continue to be a deception tool for crimes in which the victim and offender never come into physical proximity. Criminal behavior has been known to be a complex area of study; links between personality disorders and criminality may be far from simple or straightforward. Online criminal behavior has received considerable attention over the years, particularly in the field of psychology. This raises the issue of how behavior relates to personality.

Given the distinction between criminal and antisocial behavior and the continuum between behaviors and traits, there are antisocial facets of psychopathy. Psychopaths lack the ability to inhibit antisocial impulses (Foster & Trimm, 2008). At clinical levels, this impulsivity promotes criminal behavior (Hare, 1991). Psychopathy is the most aggressive and overtly criminal of the subcomponents of the DT. Researchers have determined that a psychopath’s erratic lifestyle refers to the tendency to behave impulsively and lack of self-regulatory resources (Paulhus & Williams, 2002; Williams et al., 2007). This tendency likely contributes to a proclivity for criminal behavior

(Mahmut et al., 2011). Given the robust association between psychopathy and crime (Hare, 2006), psychopathy has become one of the most important psychological constructs within the criminal justice system (Hare et al., 2000; Hare & Neumann, 2010).

Crime and deviance reflect the dynamic nature of social life. The Internet has transformed opportunities for crime and deviance, much as it has changed other aspects of social life. Although criminology recognizes the influence of numerous factors in predicting and understanding criminal behavior, historically the field has primarily focused on social factors. Criminal behavior and the individuals who commit these actions exhibit wide heterogeneity. Most crimes exhibited within SNSs can be attributed to deviance and conduct problems. Conduct problems are characterized by persistent and severe noncompliance, aggression, destructive behavior, lying, and violation of societal rules (Day et al., 2011). The dark side associated with the growth of the Internet must be contrasted with its social advantages. The pirating of digital goods, the manufacture of viruses and cyber-attacks, cyber-victimization, harassment and stalking, as well as other online deviance are all aided by computer-mediated communication (Fox et al., 2011; Holt, 2012; Holt et al., 2010; Holtfreter et al., 2008). The use of the SNSs for criminal and deviant purposes is only likely to grow as Internet access and use continues to expand. This will also propel higher threat statistics among newer (and older) generations online. Table 1 below outlines major threats and relevant research into criminal behaviors to date.

Table 1: Criminal Behaviors and Definitions

Table 1 Criminal Behaviors			
Criminal Behavior:	Definition:	Explored by:	Title:
Unethical Hacking	Unethical hacking is the unlawful act of targeting a network or system to steal information, money, or to cause damage to its targeted victims.	Jordan, T., & Taylor, P. (1998)	"A sociology of hackers."
		Campbell, Q., & Kennedy, D. M. (2009)	"The psychology of computer criminals."
		Schell, B. H., & Dodge, J. L. (2002)	"The hacking of America: Who's doing it, why, and how"
		Holt, T. J., et al. (2012)	"Examining the social networks of malware writers and hackers."
		Chiesa, Raoul et al. (2009)	"Profiling hackers: The science of criminal profiling as applied to the world of hacking"
Cyber Bullying	Cyberbullying is the illegal use of information or communication technology to harass and harm in a deliberate, repetitive, and hostile manner. Cyberbullying can be communication-based or content-based. Methods used for online bullying include name-calling, gossiping, ignoring, threatening, disseminating personal conversations, manipulating and spreading pictures, creating defamatory websites, and sending sexual comments (Dehue et al. 2008; Vandebosch and Cleemput 2008).	Goodboy, A. K., & Martin, M. M. (2015)	"The personality profile of a cyberbully: Examining the Dark Triad."
		Alhabash, S., McAlister, A. R., Hagerstrom, A., Quilliam, E. T., Rifon, N. J., & Richards, J. I. (2013)	"Between likes and shares: Effects of emotional appeal and virality on the persuasiveness of anticiberbullying messages on Facebook."
		Holt, T. J., & Bossler, A. M. (2014)	"An assessment of the current state of cybercrime scholarship."
		Luppicini, R. (2014)	"Illuminating the dark side of the internet with actor-network theory: An integrative review of current cybercrime research."

Table 1 Criminal Behaviors			
Criminal Behavior:	Definition:	Explored by:	Title:
Cyber Stalking	Cyber stalking is a crime in which persistent messages are sent to an unwilling recipient.	al-Khateeb et al. (2015)	"A practical guide to coping with cyberstalking."
		Bocij, P., & McFarlane, L. (2002a)	"Online harassment: Towards a definition of cyberstalking."
		Bocij, et al. (2002b)	"Cyberstalking: A new challenge for criminal law."
Identity Theft	The Identity Theft Resource Center (ITRC) defines identity theft as "a crime in which an impostor obtains key pieces of personal identifying information (PII) such as Social Security numbers and driver's license numbers and uses them for their own personal gain" (http://www.idtheftcenter.org/).	Smith, R. (2010)	"The handbook of internet crime."
		Reyns, B. W., & Henson, B. (2016)	"The thief with a thousand faces and the victim with none: Identifying determinants for online identity theft victimization with routine activity theory."
		Kirwan, G., & Power, A. (2012)	"Can Theories of Crime be Applied to Cybercriminal Acts?"
		Marshall, P. D., & Barbour, K. (2015)	"Making intellectual room for persona studies: a new consciousness and a shifted perspective"

2.4.1 Unethical Hacking

Unethical hacking is when skilled individuals use their abilities illegally to harm society by finding vulnerabilities in computer systems and attacking or exposing them, often by creating and distributing virus-containing or malicious software for personal gain. This behavior is considered unethical and criminal, prosecutable in accordance with U.S. laws (Sukhai, 2004). For several years, a number of studies have proposed frameworks and models to represent the determinants of unethical behavior (Bommer et al., 1987; Trevino, 1986; Ferrell and Gresham, 1985). Many past business ethical studies explore the factors that influence ethical decision-making and behavior. Most unethical behavior, such as deception and computer hacking, requires substantial resources and opportunities to perform successfully. Levy (1984) refined the term “*hacker ethic*” from the early, non-computer intruder hackers. This ethic, oftentimes elevated by all types of hackers is outlined as: all information should be free; mistrust authority, promote decentralization, and hackers should be judged by their hacking, not by false criteria such as degrees, age, race, or position (Levy, 1984, pp. 40-45). Social scientists have attempted to explore the culture and subcultures of hackers to understand the attitudes and normative values that persist within the Internet community (Holt, 2007; Jordan & Taylor, 1998).

The hacker community is characterized by an easy relationship with technology, in particular with computer and communications technology. The term hacking has evolved over the years, but in general, it refers to the use of a computer to gain unauthorized access to information systems or to exploit the weaknesses of computer networks (Holt et al., 2015). Unethical hacking is against the law, and those who engage in the act are considered cyber criminals. Currently, criminal law has split digital or cybercrime into a multitude of criminal offences. Examples are the making and/or distribution of malware, computer intrusion, illegal surveillance, interference with

computer data, interference with computer systems, computer fraud, and fraud by deception. Hackers perform premeditated threats against computers and/or networks, with the intention to cause harm; further social, ideological, religious, or political agendas; or to intimidate any person. All are criminal acts punishable by law.

In 1986 Congress passed the Computer Fraud and Abuse Act and the Electronic Communications Privacy Act, which made hacking illegal. Additionally, unethical hacking is illegal or criminal under the Computer Misuse Act of 1990. Other legislative agendas followed in years to come, outlawing acts of cybercrime.

Hackers can be characterized by their resemblance to basic personality attributes. Hackers or cybercriminals are sensation-seeking, a biologically based personality trait that motivates individuals to seek novel and intense experiences (Zuckerman, 1979). Thus, skilled hackers do not fear punishments, as society praises their technological skills despite their anti-social and unethical behaviors. In this view, the key personality attributes are what have historically been assessed as “dark.” Some case studies have suggested a relationship among personality traits, deviant behaviors, and computer hacking.

Research indicates computer hackers may exhibit individual traits associated with certain personality disorders. For example, some computer hackers may be prone to higher rates of hostility and exhibit a greater tendency for egotistical qualities (Campbell & Kennedy, 2009; Schell & Holt, 2002). Narcissism or even narcissistic personality disorder is characterized by an excessive perception of entitlement, as well as a lack of empathy, both of which are associated with some subsets of computer criminal behavior, especially insider hacking. The insider hacking or threat is always present and establishes itself in many ways. There have been exhaustive discourses on everything from what exactly an insider threat is (Hunker & Probst, 2011) and what

the range of human and psychological factors involved are (Greitzer & Hohimer, 2011), to how threats can be predicted, identified, and effectively addressed with the rise of technological and behavioral advances and theories (Nurse et al., 2014b). In addition, computer criminal deviants may exhibit low empathy, insincerity, dishonesty, and enhanced intellect, all of which are consistent with antisocial personality disorder, as individuals with the disorder do not believe their actions cause harm to others or break the law (Campbell & Kennedy, 2009). Particularly, these traits may be more likely to manifest in hackers who excel in social engineering, or the manipulation of others to obtain certain means through hacking (Chiesa et al., 2009; Kirwan & Power, 2012). An empirical study that evaluated the relationship between Internet hacking and psychopathy assessed whether or not Internet hacking was related to the DT (Williams et al., 2001).

Additional current research has examined personality correlations of specific types of computer crimes. Seigfried-Spellar and Treadway (2014) found low agreeableness predicted self-reported hacking; high scores on neuroticism and low scores on internal moral values predicted virus-writing; and low scores on internal moral values predicted identity theft. Furthermore, Seigfried-Spellar et al. (2017) found individuals who self-reported denial of service attacks (DoS) scored low on agreeableness and hedonism compared to cyber criminals who did not engage in DoS attacks. A recent study (Siegfried-Speller et al., 2015) examined whether personality characteristics associated with Asperger syndrome were significantly related to hacking, cyberbullying, identity theft, and virus-writing. Bachmann (2010) suggested that hackers who exhibit high risk-taking behaviors engage in a higher number of hacking behaviors, but with less success overall.

2.4.2 Cyberstalking

Cyberstalking involves the criminal use of electronic media to stalk or harass an unwilling individual, group, or organization in cyberspace. Cyberstalking is now more common than offline stalking, with a high percentage of victims being stalked through social networks (McVeigh, 2011). Despite decades of criminological research, there has not been a generally agreeable definition of cyberstalking. Existing definitions of cyberstalking tend to be derived from definitions of physical stalking. Bocij et al. (2002) believe cyberstalking should be regarded as an entirely new form of deviant behavior and make distinctions between conventional stalking and cyberstalking. Bocij and McFarlane (2003) offered a more comprehensive definition:

“A group of behaviors in which an individual, group of individuals, or organization uses information technology to harass one or more individuals. Such behavior may include, but are not limited to, the transmission of threats and false accusations, identity theft, data theft, damage to data or equipment, and computer monitoring...”

The definition encompasses a large number of deviant behaviors, which vary by nature and require different approaches. In an earlier study, Meloy (2001) provided a more condensed definition, which asserts cyberstalking as consisting of two major roles: a) the stalker gathers private information of the target to further a pursuit and b) the cyberstalker communicates with the target to implicitly or explicitly threaten or to induce fear. It is the stalker’s ability to collect personal information of the victim that places the victim in the danger of threats and harassment. Currently, there is currently no formal profile of a cyberstalker (Barnes, 2013), especially for specific subtypes of cyberstalking. Burmerster et al. (2005) point out that cyberstalking is very difficult to profile, as it involves complex and sometimes unpredictable behaviors.

Cyberstalking overlaps considerably with similar behaviors such as cyberbullying, cyber harassment, and “trolling.” All three types of deviant behaviors have become prevalent problems that are associated with SNSs, and have serious social and psychological implications, which

hinder the safe usage of the Internet (al-Khateeb et al., 2015; Pittaro, 2007). Cyberstalking is differentiated from cyber harassment because it continues over a more prolonged period of time and from trolling in that it is targeted toward a specific person or persons (Ogilvie, 2000; Sheridan & Grant, 2007).

In the last decade, there have been major initiatives to improve the detection of phishing, spamming, cloning, and bots on SNSs (Fire et al., 2014). No technical breakthrough specifically focusing on cyberstalking has been found. There is a lack of emphasis on behaviors and paucity of research on cyber vs. overt stalking, and much of it has been conducted with stalking victims rather than offenders (Pittaro, 2007). This may be because of the multifaceted nature of the online user interactions and the actions generally associated with cyberstalking, such as online harassment and identity theft.

In the absence of information from epidemiological surveys, information about the nature of cyberstalking has largely been drawn from college-student samples or samples of self-identified stalking victims. Cyberstalking manifestations may include anger, control, and revenge (Davis et al., 2000). In a traditional stalking literature, Gothard and Meloy (1995) found that 85% of their sample qualified for a personality disorder diagnosis, including antisocial, schizoid, borderline, avoidant, paranoid, and personality disorders not otherwise specified. According to Meloy (2001), the most common diagnosis of male stalkers is antisocial personality disorder, followed by narcissistic personality disorder. Mullen and colleagues (2001) suggest that between 30% and 50% of participants in clinical samples have personality disorders and Meloy (1998) refers to stalkers as “narcissists” (p. 18). A study by Alexy et al. (2005) found some differences between those who were subject to on-line vs. overt means of stalking. The authors speculate that cyberstalking may permit the offenders to be more “histrionic” in their behavior. That is, cyber stalkers may behave

in a more dramatic manner, because they are not in physical proximity of their victims, and so do not need to act on their “threats.” Furthermore, Alexy et al. indicate that more men were actually victims of cyber stalking.

Interestingly, the cyberstalking phenomenon is a perverse example of DT manifestation. In addition to gender, the association between dark personality traits also has been explored by research (the Dark Tetrad; Chabrol et al., 2009), as well as the perpetration of stalking behaviors (Ménard & Pincus, 2012; Storey et al., 2009). Jones & Paulhus (2010) and previous research have suggested narcissism plays a key role in stalking behaviors. The deceptive and manipulative behavior of the Machiavellian traits can be considered synonymous with the covert, deceitful nature of cyberstalking (Sheridan & Grant, 2007). Research has found an association between measures of psychopathic personality disorder and stalking behaviors, thus directly linking trait psychopathy with stalking (Kropp et al., 2011; Storey et al., 2009).

To date, deviant behaviors identified as cyberstalking include but are not limited to: repeated unwanted emails or instant messages, posting false or misleading information about victims online, using SNSs to harass the victim, subscribing to services or products in the victim’s name, hacking into victim’s personal accounts, virtual identity theft, impersonating the victim online, spamming or distributing computer viruses, and recruiting others to harass or threaten the victim via the Internet (Sheridan & Grant, 2007).

2.4.3 Cyberbullying

The convergence and the progression of new social media (e.g., instant messaging, Facebook, Twitter, Instagram) have given aggressors a “new” method to cause harm, termed *cyberbullying*. Research has shown that the probability of being involved in cyberbullying is

predicted by time spent online (Hinduja & Patchin, 2008), particularly time spent on SNSs (Lindsay & Krysik, 2012).

Cyberbullying is an umbrella term related to similar constructs such as online bullying, electronic bullying, and Internet harassment. Several definitions of cyberbullying exist; most are predicated on accepted definitions for traditional bullying. Dehue et al. (2008) suggest that three necessary conditions must be met for a situation to be considered cyberbullying: the behaviors must be repeated, involve psychological torment, and be executed with malevolent intent. Therefore, cyberbullying can be appropriately defined as any behavior performed through electronic or digital media by individuals or groups that repeatedly communicates hostile or aggressive messages intended to inflict harm or discomfort on others (Tokunaga, 2010).

Cyberbullying victimization is one such offense that has received increased attention from scholars and practitioners. Cyberbullying can be viewed through the lens of individual differences that are psychological traits or chronic tendencies that “convey a sense of consistency, internal causality, and personal distinctiveness” (Carver & Scheier, 2000, p. 5). As Menesini and Spiel (2012) stated, “Although some consistent findings have been reached so far, there is still a lack of knowledge about developmental processes of cyberbullying and on possible predictors and correlates, such as personality” (p. 164). Most cyberbullies spend a considerable amount of time online and engage in risky online deviant behaviors, but there are important individual personality differences that predict this behavior beyond characteristics of Internet use (Görzig & Olafsson, 2013). A recent study examined the relationships between the DT personality traits and self-reported cyberbullying behaviors (Goodboy & Martin, 2015). In a different study, Fanti et al. (2012) found that narcissism, traditional bullying, and cyber-victimization predicted cyberbullying frequency. Manipulation is an often underconsidered form of bullying, but unfortunately there

have been many cases of manipulative cyberbullying. Individuals who display more Machiavellian traits are characterized by cold and manipulative behaviors (Christie & Geis, 1970) and engage in deviant behaviors or other forms of aggression to gain or maintain influence over others. These individuals have been characterized as having the “darkest” of the DT personalities (Rauthmann & Kolar, 2012). In relation to cyberbullying, social-group manipulation can be accomplished through relatively anonymous threats of real-world aggression or cyber-aggression.

In the case of cyberbullying, the act itself may cause repeated victimization because the threat actor relies upon Internet users to spread the original posting to other websites or SNSs. A cyberbully can act anonymously and spread malicious offenses over the Internet to reach a potentially unlimited audience, distributing viruses, spyware, and hacking programs to their victims. Trojan programs allow the cyberbully to control their victim’s computer remotely and can be used to erase or steal personal information from the hard drive of the victim. Other behaviors such as virtual identity theft is not included in traditional forms of bullying but are considered as cyberbullying (Perren et al., 2012). Since the process of cyberbullying remains unclear to a large extent, the application of existing theoretical formulations used in predicting human behavior would be a good starting point.

Cyber-bullies appear to possess highly advanced technical skills and use the Internet more frequently, while they also seem to be more skilled in other forms of violence (Turan et al., 2011). Barlett and Gentile (2012) posited that, through learning mechanisms, cyber-bullies likely learn that there are often little immediate consequences for an online aggressor. In most cases, if hacking or identity theft is involved, it can be a serious criminal matter under state and federal law.

2.4.4 Identity Theft

In 1998, Congress passed the Identity Theft Assumption and Deterrence Act (the Identity Theft Act; U.S. Public Law 105-318). This act identifies offenders as anyone who

... knowingly transfers or uses, without lawful authority, any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law.

While identity theft may seem innocuous, the catastrophic impact it could have on the victims of this crime could lead to irreparable loss to the individual or family, damage to reputation and destruction of careers, and in some cases can lead to loss of life stemming from extreme stress caused by the consequences of this cybercrime.

Something extraordinary has shifted in recent years that has led to an intensive focus on constructing strategic masks of identity. The catalyst is the development of online culture and its high demand to personalize the expression of a public self – essentially a persona – regularly and incessantly (Marshall & Barbour, 2015). As mentioned, the term personality is derived from the Latin word *persona*; which means *mask* (Burger, 1993). Thus, it can be said that the study of personality can be understood as the study of *unique masks that people wear*. Accordingly, the theft of one's social identity is a risky form of malicious masquerading. Empirical studies of identity-theft victimization have published evidence suggesting that identity theft continues to be a growing problem (Langton & Baum, 2010; Smith, 2010). Identifying which SNS users are most likely to perpetuate it is another growing concern.

Past research suggests that aggrandized and deceiving self-presentations are more likely to appear when targeted audiences are comprised of relative strangers that lack knowledge of the source, relative to audiences who have little knowledge of the source (e.g., friends). Some people form their self-concepts partially based on their relationships with or membership in certain social

circles, which may be referred to as social identity (Tajfel & Turner, 1986), and this leads to affective commitment, which is a form of psychological attachment to others with whom one identifies (Allen & Meyer, 1990). Social identity–related misuse represents a significant threat to the fabric of our existence (Neuman, 1997). More specifically, an attacker can easily mimic the SNS profile data of a user to create an identity on other SNSs, such as Facebook, Twitter, Instagram, or Google+. These social identity accounts are known as “doppelgangers,” eerie doubles or look-alikes. Doppelgangers highlight unwanted exposure to privacy vulnerabilities. There have been several incidents of hackers registering a new account under the name of celebrities or regular SNS users. In a recent study, Goga et al. (2015) found that most identity doppelganger attacks are not targeting celebrities; they instead clone the profiles of ordinary people on Twitter to create real-looking fake identities and use them in malevolent activities such as follower fraud. Such a fake account can be used to spread misinformation and rumors or to attract new followers that can later be victims of social-engineering attacks.

Malevolent attackers (cyber criminals) are known to use *Sybil* identities to post spam content and to tamper with the popularity of content on SNS sites (Viswanath et al., 2014). Sybil attacks (Douceur, 2002) are harmful attacks where someone or something illegitimately claims multiple identities. Consequently, a number of preceding works have focused on understanding and detecting Sybil attacks in online social networks (Mislove et al., 2008; Mondal et al., 2012; Molavi et al., 2013).

Cyber criminals do not need to access someone’s account details to impersonate them. As more personal data about users becomes publicly available on the Internet, identity or impersonation attacks become easier to carry out.

2.5 Theoretical Framing

SNSs are used across many or most social boundaries; therefore, it is a logical area to investigate from a personality and behavioral perspective, particularly since the level of usage is often unrestricted and self-driven rather than mandated, and thus more probable to reflect personal motives, desires, beliefs, preferences, and other personality traits.

Sledgianowski & Kulviwat (2009) argue that a SNS is a pleasure-oriented hedonic information system; their study is limited in context to social networking websites and hedonic information systems. Thus, attribution theory (Heider, 1958), a hedonic or pleasure motivation theory, is used. Hedonic or pleasure motivation theories are the largest category of motivational theories. The categorization of motivation theories is an attestation to the complexity of the phenomenon. Motivation theories seek to explain the driving forces that transform our thoughts into behaviors. There are various theories of motivation, where each either explains the same motivational concept with different verbiage or proposes a new motivational theory. The attribution theory attempts to explain behaviors by indicating a cause. Weiner (1980) suggests that attribution encompasses a three-stage process: 1) behaviors are observable, 2) behaviors are deliberate, and 3) behaviors are attributed to either an internal or external cause. According to Heider (1958), attributions (causes of behavior) are based on two sources of information:

- *Internal (dispositional) attributions* – based on something within the individual whose behavior is being observed; the individual's natural character (i.e., personality).
- *External (situational) attributions* – based on something external to that individual, based on their circumstances and surroundings.

2.5.1 Attribution Theory

An extensive amount of research has been conducted on the psychological processes that underlie how one's behavior is perceived by others, collectively referred to as attribution theory. Such research has largely been guided by the covariation principle (Kelley, 1967) and the disposition or situation attribution distinction that formed the actor-observer asymmetry (Jones & Nisbett, 1971). Attribution theory posed questions and highlighted phenomena that had not been considered before – such as the power of behavior explanations (Heider, 1958; Jones et al., 1972), actor-observer differences (Jones & Nisbett, 1971), self-serving bias (Bradley, 1978; Miller & Ross, 1975; Heider, 1958), and consequences of behavior explanations (Anderson et al., 1996). Despite the lengthy history of attribution research, it has been met with criticisms at the conceptual level (Buss, 1978), particularly regarding its application to the computer-mediated communication phenomena (Bazarova & Hancock, 2010; Spitzberg & Manusov, 2014). Osgood et al. (1996) argued that when individuals spend time engaged in unstructured and unsupervised socializing with peers, it provides natural situational opportunities for deviance.

Applying the attribution theory to cyberspace, the act of criminality or criminal behavior might be attributed to a situational factor and/or a dispositional factor, like the unethical attitude or behavior of a perpetrator (Levin et al., 2004). Attributions are the ways people explain their own or others' behavior: how they see its causes, and whom they consider responsible. Internal (dispositional) causes are factors within an individual; external (situational) causes are in the situation or environment. Social psychologists have been interested in attribution errors, such as the “actor-observer bias” (Jones & Nisbett, 1972) in explaining negative events. The actor-observer bias is a term in social psychology that refers to a tendency to attribute one's own actions to external causes, while attributing other people's behaviors to internal causes. The actor-observer

bias tends to be more noticeable in situations where the consequences are negative. This research attributes the negative events caused by the disposition of the actor to infer a situational cause for the observer. For example, in trying to infer intentions, people often fall victim to the fundamental-attribution error (Fiske & Taylor, 2013). Thus, intentions are directly inferred from observable human actions because “the most cognitively available explanation for behavior is some intrinsic property or disposition of the person who performed the behavior” (Tetlock & McGuire, 1986, p. 163). Based on this logic, threat actors appear aggressive by nature, and not through misunderstandings or adverse situations.

To date, there is no IS research in which attribution theory is applied to understand the influence that cybercriminals have on SNSs using the DT personality traits. The prospect of finding a non-technical solution to the technical process of attribution is overwhelming because cyber criminality is not only a technical pursuit, it also exhibits human behavior.

Attribution theory, glossed in Figure 1 below, has occupied a major role in social-psychological research. Unfortunately, the term *attribution* is abstruse. According to one meaning, forming an attribution is *making a dispositional (trait) inference* from behavior; according to another meaning, forming an attribution is *explaining* behavior (Hamilton, 1998; Malle, 2004). The focus of this study and research model is on the latter phenomenon of behavior explanations, more specifically criminal behaviors. More research needs to be carried out to test the validity of attribution theory in predicting criminal behavior. Further, this research asserts that there is a need to examine and critically evaluate what factors lie beneath criminal behaviors among SNS audiences.

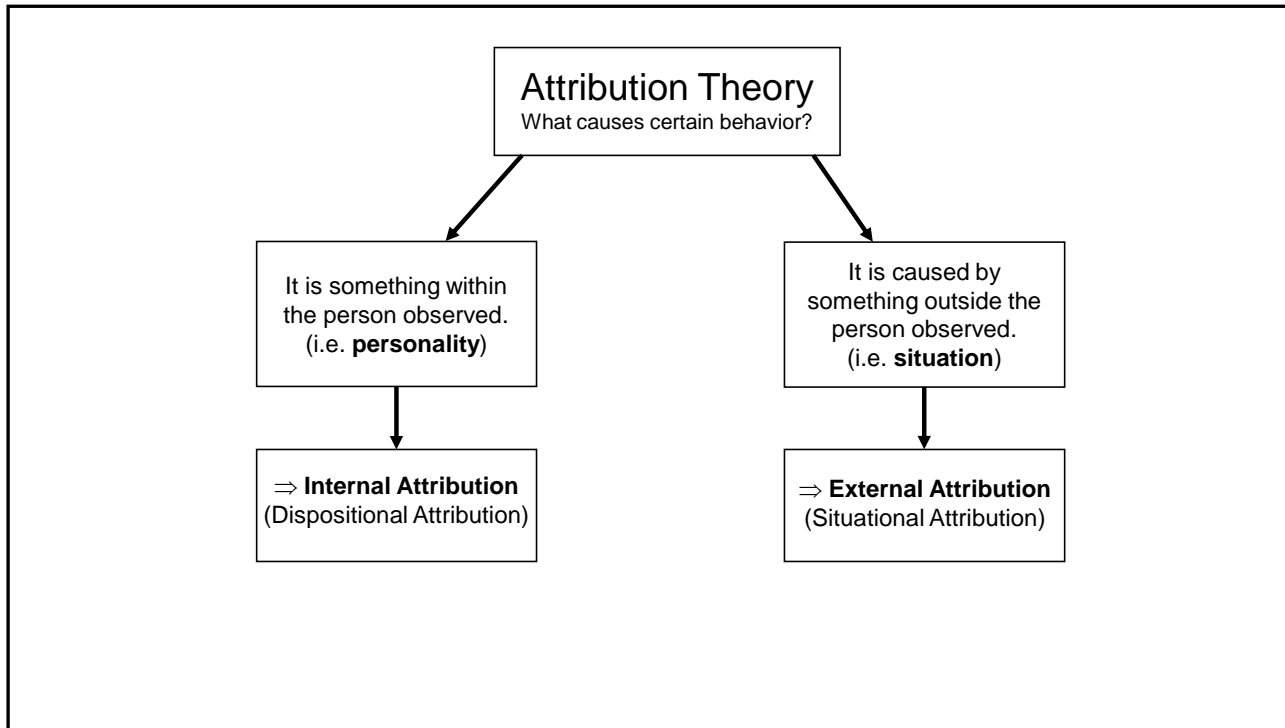


Figure 1: *Attribution Model (Heider, 1958)*

Eisenhart (1991) defined a theoretical framework as “a structure that guides research by relying on a formal theory ... constructed by using an established, coherent explanation of certain phenomena and relationships” (1991, p. 205). The psychosocial behavior attribution model developed in this study is based on the attribution theoretical framework depicted in Figure 1. The theoretical framework in Figure 2 extends the attribution theory as an alternative explanation to the SNS cyber threat landscape, by examining the threat actor through the lens of DT personality traits and criminal behaviors. Figure 2 shows that there is a relationship between DT personality traits and criminal behaviors. This research suggests that personality drives behavior within individuals, correlating personality traits (dispositional attribution) to that of criminal behaviors, within the realm of SNSs (external attribution).

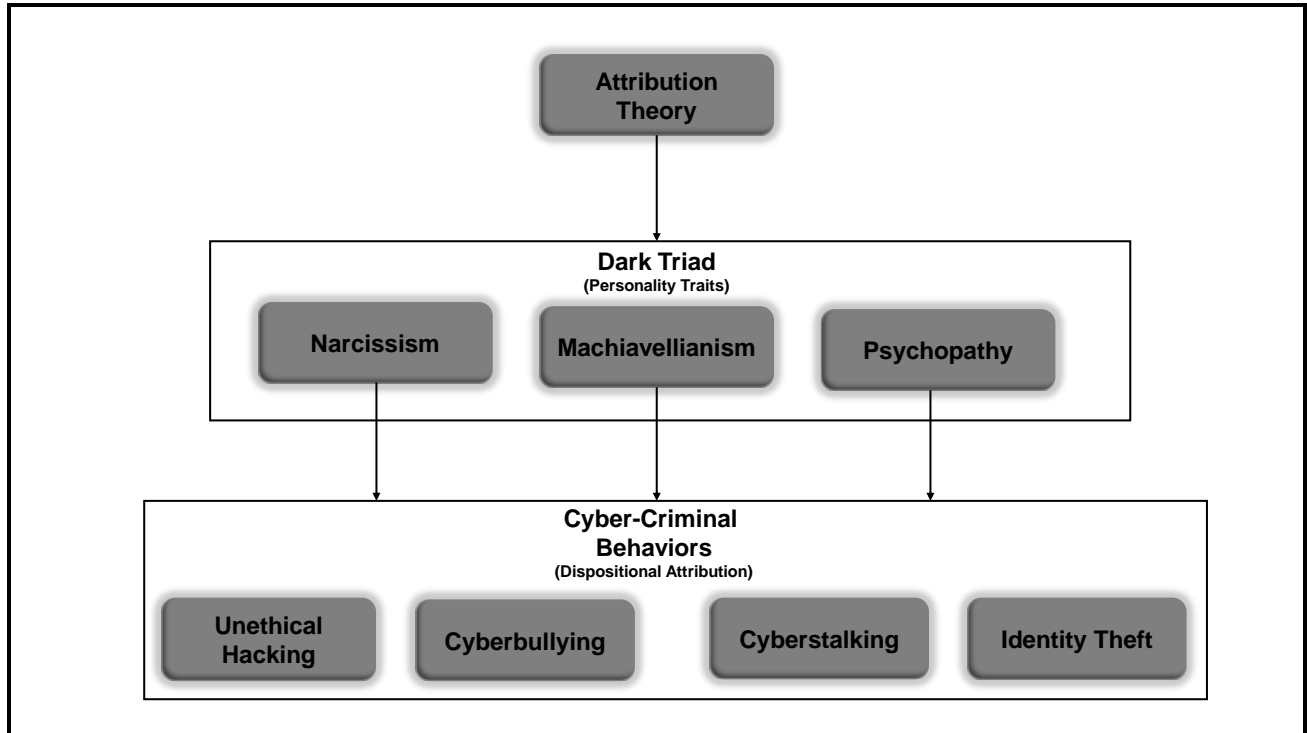


Figure 2: *Psychosocial and Behavioral Attribution Model*

Prior personality models have been proposed in literature. One of them use multiple indicators, such as personality traits and verbal behavior, so as to be able to predict insider threats (Schultz, 2002). Parrish et al. (2009) proposed a conceptual framework that utilizes the Big Five personality traits as a possible way to explain why some people are more susceptible than others to phishing attacks. Further, researchers assert personal or individual factors are constant constructs that imitate personality traits, thoughts, and inherited predispositions (Scheuer, 2010). In brief, there is a lack of understanding of why personality traits or individual-related factors should be predictors of various forms of malevolent or criminal behavior on SNSs.

2.5.2 Conceptual Model

The measurement of human behavior belongs to the widely accepted positivist view, or empirical analytic approach, to discern reality (Smallbone & Quinton, 2004). Because most

behavioral research takes place within this paradigm, measurement instruments must be valid and reliable. This study intends to explore DT constructs within SNSs and the negative effects on SNSs and their many users; additional data-driven perspectives are necessary to distinguish reliability and validity. Specific characteristics including age, gender, and knowledge of online habits are analyzed to determine their impact on the participant's ability to identify legitimate threat-carrying correspondence.

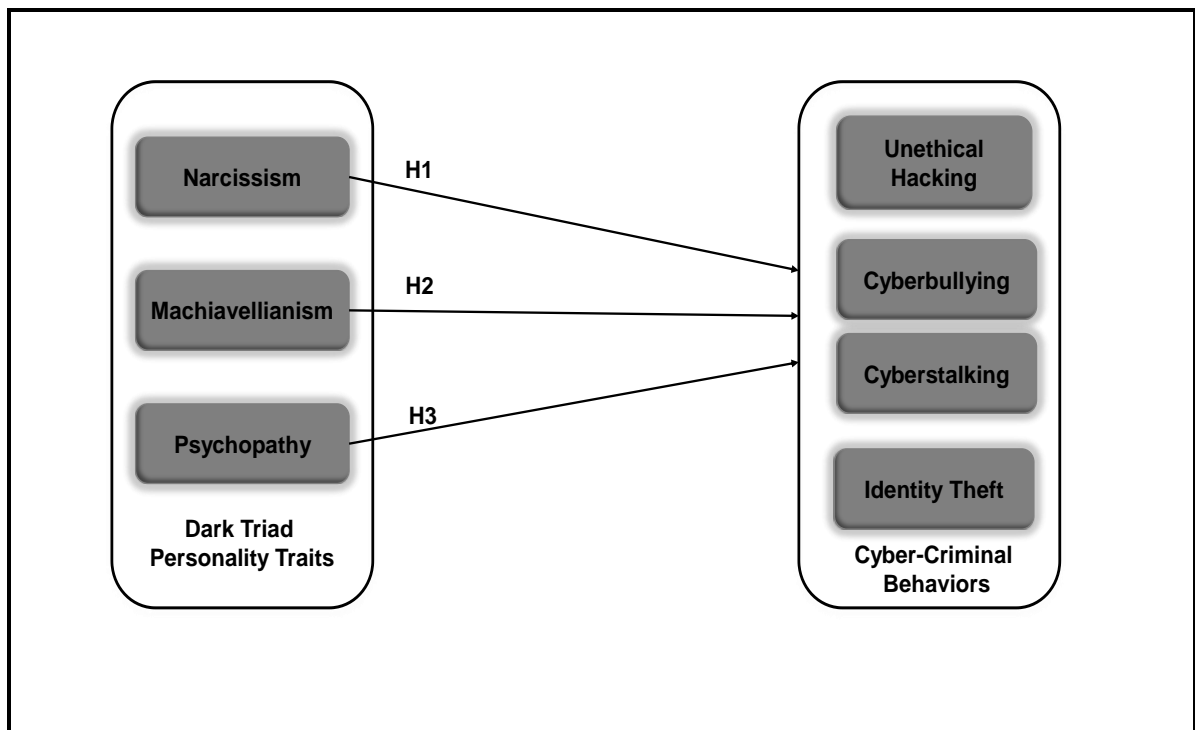


Figure 3: *Conceptual Model*

2.5.3 Hypotheses

This study is embedded in a much broader conceptual framework of personality description and social environmental influences, which is meant to test the proposed psychosocial behavioral model. It is also important to identify which, if any, personality characteristics are predictive of engagement in criminal behaviors. It is hypothesized that the DT is predictive of engagement in cyber-criminal behavior.

Based on the evidence linking these personality traits to aggressive behavior, it is hypothesized that the DT traits Machiavellianism (Hypothesis 1), narcissism (Hypothesis 2), and psychopathy (Hypothesis 3) will predict criminal behaviors. Based on the attribution theory's dispositional attributions, wherein human behavior is attributed to personality traits, the following hypotheses are tested:

H₁: There is a positive relationship between narcissism and one or more of the cyber-criminal behaviors depicted in Figure 3.

H₂: There is a positive relationship between Machiavellianism and one or more of the cyber-criminal behaviors depicted in Figure 3.

H₃: There is a positive relationship between psychopathy and one or more of the cyber-criminal behaviors depicted in Figure 3.

The research summarized in this paper suggests that some micro- and macro-level factors should be considered in the context of online deviance. Particularly among SSNs, the Internet has facilitated new opportunities for deviance, such as the development of viruses, malware, cyber terrorism, hacking, online harassment, and certain self-harm behaviors (Joinson, 2005).

According to the cognitive development theory (Moore, 2011), criminal and deviant behavior results from the way in which individuals organize their thoughts around morality and the law. Sigmund Freud (1923) states that all humans have natural drives and urges that are repressed in the unconscious and that all humans have criminal tendencies.

2.6 Summary

The literature has been extensively reviewed on the concepts and theories related to cybercrime and criminal behaviors. Further, the review of primarily research papers or articles and other acknowledged related work in the fields of psychology and criminology has been examined. The scope of topics included in the research ranged across cyber security, cybercrime, cyber laws,

impact of cyber security rules, and regulations developed by government entities. The review of available literature on each topic is considered in this chapter.

Additionally, this chapter addressed the theoretical framework and the research method approach for this study. The theoretical framework contains the analysis of the underlying principles inherent in attribution theory and the construction of the relationship between personality and cyber-criminal behaviors. The framework also provides the descriptions of the constructs, the hypotheses, the conceptual model, and the philosophical position of this study.

Chapter 3

Methodology

3.1 Introduction

This chapter is divided into seven sections, which provides an overview of the methodological structure of this study. The second section is an overview of the research design. The third section provides an overview of the survey sample and procedures used. The fourth section provides an overview of the measurement model, constructs, instruments, reliability, and validity. The fifth section provides the structural model approach of this study. The sixth section provides an overview of common method variance and outlines the remedies used. Finally, section seven summarizes the chapter.

3.2 Research Design

Researchers on Dark Triad characteristics have exclusively employed cross-sectional approaches to explore associations among narcissism, Machiavellianism, and psychopathy, and with psychosocial outcomes (Muris et al., 2017). For this reason, this study was implemented using a cross-sectional quantitative survey.

Data was collected using the Qualtrics online survey platform (Qualtrics, 2018). Given the nature of the conceptual model and the exploratory nature of this research, this study used partial least squares structured equation modeling (PLS-SEM) for the analysis (Hair et al., 2017). PLS-SEM is an accepted method within the information systems discipline, cyber-psychology discipline (Charoensukmongkol, 2016; Fischbacher-Smith, 2015), and cyber-criminology discipline (Zhang et al., 2016; Riek et al., 2014). Many researchers advocate the use of SEM as

the most robust tool to assess a test's reliability, mainly because it allows one to specify and compare different models of reliability (Green & Yang, 2011; Graham, 2006).

This analysis began with an evaluation of the measurement model to ensure the suitability of the targeted constructs, followed by an evaluation of the structural model necessary to support the hypotheses of this study (Gefen et al., 2011; Hair et al., 2017). The framework and nature of this study was more exploratory than confirmatory. Therefore, PLS-SEM was the most suitable analysis technique for this current research.

In PLS-SEM, the minimum sample size should be compared to the complexity of the structural model. Notably, PLS-SEM is suitable when measurement models have a few indicators, less than six, or the sample size is greater than 100 (Hair et al., 2017). The minimum sample size should be no less than ten times the number of formative measurement indicators of a single construct or ten times the largest number of structural paths directed at a particular construct in the structural model (Hair et al., 2017). Based on these criteria, this study sought to acquire a sample size of at least 120 observations.

3.3 Survey Sample and Procedures

A survey was conducted targeting individuals with hacking experiences or within hacking communities as the population being studied. Notably, hackers are not inherently bad; the word "hacker" does not definitively mean "criminal." The definition of the word "hacker" is controversial and could mean either someone who compromises computer security or a skilled developer in the free or open-source software movements (Hoffman, 2013). Therefore, the target population primarily was focused on offensive security researchers or engineers. Offensive security engineers are justified in their hacking behaviors, which will eliminate self-report bias of criminal behavior. Offensive security engineers utilize hacking techniques to perform their daily

job functions. For several years, the U.S. military has employed offensive security engineers to attack cyber adversaries using potent cyber weapons or cyber tools that can break into enemy computers (Gjelten, 2013). Offensive security techniques have been trending in the hacker communities and have since spread to business communities and social media platforms such as Facebook.

This particular method of sampling focuses on the skill set of the individuals within the hacker community, rather than their intentions. To sample from this population with a probabilistic sampling technique would be difficult given the small proportion of computer deviants to non-computer deviants and the high risk associated with disclosing criminal information (Loper, 2001; Rogers, 1999, 2006). Sampling from a general population of computer users or non-computer deviants may not render the intended responses based on the content of the survey instrument.

Because the study is intended to reach a difficult demographic to survey, the study utilized the snowball sampling strategy (Hagan, 2010). This technique is appropriate to this study given that offensive acts in the cyber domain raise a host of legal, ethical, and political issues in governments, court systems, and business (Gjelten, 2013).

All survey items were adapted from previously validated instruments wherever possible (Boudreau et al., 2001). The web-based survey instrument was hosted on Qualtrics®. Qualtrics is a tool for maintaining regulatory mandates for confidentiality in data collection. Qualtrics aids in acquiring the user's data and maintaining regulatory standards of practice of confidentiality. In addition to the web-based survey link, quick response (QR) codes were distributed electronically (see Appendix E). QR codes are becoming more common with mobile and smartphone technologies. Like the barcodes on consumer goods, the QR code is a machine-readable label that contains data, in this case the survey URL. Prior to filling out the survey, the respondents were provided a participation consent page (see Appendix D), which informed them of the purpose and

potential risks of the study, and provides necessary contact information for the university and researchers. Ethical mandates provided by the Institutional Review Board (IRB) (see Appendix F) were met prior to the start of the survey activity.

Recruiting the subjects began with advertisements of the survey along with a short informative introduction letter (see Appendix E) in targeted popular forums, chat rooms, and Facebook pages where hackers are known to congregate. This sample focused on soliciting individuals online with tenuous ties to hacker culture (e.g., white hats, red hats, black hats, gray hats), though they may have similar hacking skills. Other methods of recruitment were via e-mail distribution and printed flyers.

Additional respondents have been identified based on solicitations made at hacker conventions, online groups, and other hacker communities within the SNSs. Many hackers exist within social groups (e.g., LinkedIn, online hacker forums, Black Hat/DefCon, Hacker List) that provide expertise, support, training, journals, and conferences, and this self-identification made them ideal for recruitment.

A “thank you” splash page (see Appendix A) at the end of the survey asked subjects to recommend the survey to friends, creating a self-perpetuating sample in accordance with the snowball sampling technique (Hagan, 2010). All sample subjects were asked to recruit people from their environment who would be willing to take part in the study. Combining these samples can provide important insights into differences among sub-populations within the hacker community. The same survey given to the computer deviant population (combatants) was also given to a general population users (noncombatants) within social networking platforms. Notably, many of the participants solicited via security conferences or hacking conferences seemed to feel more comfortable with taking the survey in person. In the end, 314 total responses were rendered. Of

that number, 62 of the combatants failed to complete the survey and 17 noncombatants responded, leaving 235 usable responses.

3.4 Measurement Model

The survey instrument is broken into three parts. The first part contained the modified Computer Crime Index-Revised Plus (CCI-R+) (Siegfried-Speller et al., In progress), which identifies the dependent variable of criminal-behavior categories. An additional cyberstalking survey adapted from research was merged with the dependent variable of criminal behaviors. The CCI-R+ scale was placed first as it is the most essential component of the study. The second part of the survey contained the independent scale that measured the Dark Triad personality traits. The final part of the survey contained the demographic variables.

The measurement constructs of this study were adopted from previously established and validated instruments. Minor sentence structures were modified as recommended based on prior research. The following section details each measurement construct, lists its source, and gives support for the mode of measurement chosen. A detailed listing of all survey questions is provided in Appendix A.

3.4.1 Independent Constructs

The primary independent variable of this study is the Dark Triad (DT). Personality researchers Jonason and Webster (2010) published a consolidated tool for measuring all three Dark Triad traits in a single instrument called The Dark Triad Dirty Dozen (DTDD). The 12-item DTDD (Jonason & Webster, 2010) has been shown to have internal consistency and test–retest reliability, and construct and convergent validity (Jonason et al., 2013; Jonason & Luévano, 2013; Jonason & McCain, 2012; Jonason & Webster, 2010). The tool contains 12 of the most reliable and representative items pulled from the NPI (narcissism), PPI-R (psychopathy), and MACH-IV

(Machiavellianism) personality tools. The DTDD instrument (see Appendix A) is a concise measure of the traits pertaining to the three Dark Triad personality traits including narcissism (four items), Machiavellianism (four items), and psychopathy (four items). The DTDD scale has been validated in several works (Kajonius et al., 2016; Jonason et al., 2011; Jonason & Webster, 2012). In their initial analysis of these traits, Paulhus and Williams (2002) reported small to moderate correlations among the three variables, as well as unique associations between each of the DT traits. In doing so, they showed the DT traits to be overlapping but still very much distinct constructs. As a result, the three DTDD dimensions are conceptualized as separate constructs: *narcissism (NARC)*, *Machiavellianism (MACH)*, and *psychopathy (PSYCH)*.

3.4.2 Dependent Constructs

Cyber-Criminal Behaviors (CCBs). Behaviors become crimes through a process of social construction. Cyber-criminal behaviors are the dependent factors of this model. Many theories have common traits, but differences among them still exist. Understanding these differences is key to understanding the often contradictory views of crime and deviance they attempt to explain. A key point in this study is whether criminal behaviors are a downstream correlate of the DT traits. The CCI-R+ was used to assess the respondent's propensity to engage in deviant or criminal behaviors with computers. Specifically, each item represents a participant's given behavior, and the respondent was asked to indicate the number of times they have engaged in that behavior. The CCI-R+ (see Appendix A) includes 29 items referencing different types of computer misbehavior ranging from less serious acts (e.g., guessing passwords) to more serious acts (e.g., identity impersonation without permission to conduct online transactions).

A coding scheme is used from previous research assessing computer-deviant behavior (Seigfried-Spellar et al., 2015; Seigfried-Spellar & Treadway, 2014). Based on item response,

respondents were classified as combatants or non-combatants. For instance, an individual who engaged in unethical hacking behaviors (i.e., hackers, cyberbullies, identity thieves, and/or virus writers) was classified as combatants (0) and individuals who did not self-report computer-deviant behaviors were classified as non-combatants (1). The following statements are examples from the CCI-R+, which were used as constructs to categorize the respondents' computer criminal behavior:

Cyberbullying (CYBU) – is conceptualized as knowingly harassing, annoying, or stalking someone using e-mails, social media, or other forms of technology.

Unethical Hacking (UH) – is conceptualized as knowingly accessing a computer system or network without authorization.

Identity theft (IDTH) – is conceptualized as knowingly electronically obtaining another person's credit-card information without permission.

The format of the CCI-R+ questions was taken largely from studies conducted by Skinner & Fream (1997) and by Rogers (2001). Skinner and Fream (1997) explored the use of social-learning theory to explain computer abuse. Rogers (2001) compared self-report survey results from known computer criminals and non-criminal Internet users. In his surveys, Rogers (2001) included questions that tested for differential association and differential reinforcement (i.e., social-learning theory), along with a number of different deviant computer behaviors.

Cyberstalking (CYST). This construct was adopted based on cyberstalking research (Lowry et al., 2013). The construct in use conceptualizes cyberstalking as one's tendency to engage in stalking behaviors using computers. Specifically, each item represented a participant's given behavior, and the respondent was asked to indicate the number of times they have engaged in that behavior. Lowry et al. (2013) introduced a theoretical model to explain and predict cyberstalking behavior. Based on an extensive review of the literature and case studies of cyberstalking, Lowry

et al. (2013) proposed a comprehensive taxonomy of cyberstalking. The cyberstalking survey instrument (see Appendix A) for this study was adapted from Lowry et al.'s research. The instrument includes 21 items referencing different types of computer misbehavior within social media. Because the cyberstalking items for this instrument has not been validated, primary concern is construct validity of the survey items.

A factor analysis of the instrument was conducted and shown in Chapter 4. For this study, since the sample size was greater than 100, factor loadings above 0.50 are considered significant (Hair et al., 1998, p.112). CFA and PLS-SEM were employed to explore the causal relationship between the tasks within each of the cyberstalking factors. Confirmatory model-testing approach by model trimming (Brown, 2006; Kline, 2005) was used to determine "model fit." Using PLS-SEM, individual item reliability was assessed by examining the factor loadings (or simple correlations) of the measures with their respective construct.

3.4.3 Factorial Validity Assessment

To demonstrate factorial validity for measurement items, it was necessary to demonstrate that a measurement item acceptably correlated with its intended construct (i.e., convergent validity) and correlates weakly (i.e., discriminant validity) with the other constructs in the research model. SmartPLS was used to perform CFA to assess factorial validity (Gefen & Straub, 2005). All measurement items used in this study were reflective.

Convergent validity was demonstrated when the outer model loadings for the items have a t -statistic of >1.96 (Gefen & Straub, 2005). Upon inspection of the t -statistics for each item, the evidence supports a claim of convergent validity if the t -statistic is >1.96 . Otherwise, items lacking convergent validity were dropped from all further analyses and re-executed.

A multi-group analysis (PLS-MGA) is used to test if pre-defined data groups have significant differences in their group-specific parameter estimates (e.g., outer weights, outer loadings and path coefficients). PLS-MGA, building on PLS-SEM bootstrapping results, is a non-parametric significance test for the difference of group-specific results (Sarstedt et al., 2011; Hair et al., 2018). A result is significant at the 5% probability of error level, if the p-value is smaller than 0.05 or larger than 0.95 for a certain difference of group-specific path coefficients. The PLS-MGA method (Henseler et al., 2009), is an extension of the original non-parametric Henseler's MGA method (e.g., Sarstedt et al., 2011).

3.4.4 Discriminant Validity Assessment

Discriminant validity ensures that a construct measure is empirically unique and represents phenomena of interest that other measures in a structural equation model do not capture (Hair et al., 2010). Discriminant validity assessment has become a generally accepted prerequisite for analyzing relationships between latent variables. For PLS-SEM, the Fornell-Larcker criterion and the examination of cross-loadings are the dominant approaches for evaluating discriminant validity.

By means of a simulation study, Hair et al. (2015) show that the Fornell-Larcker approach does not reliably detect the lack of discriminant validity in common research situations. Therefore, this study took an alternative approach, based on the multitrait-multimethod matrix, to assess discriminant validity: the heterotrait-monotrait (HTMT) ratio of correlations examined in Chapter 4.

3.4.5 Reliability

This study used Cronbach's *alpha* (α), CFA construct reliability calculations to validate the reliability of the data and the findings. CFA was utilized instead of exploratory factor analysis

because the factor structure of all the constructs was known. In CFA, the reliability of a latent variable is said to be valid if the composite reliability is greater than the average variance extracted (AVE). The AVE “measures the percent of variance captured by a construct by showing the ratio of the sum of the variance captured by the construct and measurement variance” (Straub et al., 2004, p. 424).

Cronbach’s α for each latent variable was measured. Alphas are widely used because influential texts have suggested that they are necessary and perhaps sufficient to assess reliability. John and Soto (2007) suggested that whenever a multi-item scale is administered, Cronbach’s α can be easily calculated. Nunnally and Bernstein (1994) states that alphas below 0.70 indicate poor reliability and imply poor predictive validity. It is recommended that a coefficient of at least 0.70 is required to ensure sufficient reliability, and that 0.80 or higher is preferred. Prior literature also has suggested the use of composite reliability as a replacement (Hair et al., 2014; Bagozzi & Yi, 1988). By using composite reliability scores, such values were shown to be larger than 0.60, proving reliability.

3.4.6 Validity

This study tests for construct validity because it is relevant to the potential research findings. Construct validity refers to how well you translated or transformed a concept, idea, or behavior (i.e., a construct) into a functioning and operating reality, the operationalization (Trochim, 2006). Sekaran and Bougie (2009) described construct validity as one that “testifies to how well the results obtained from the use of the measure fit the theories around which the test was designed” (p. 436).

Convergent validity is shown when each measurement item correlates strongly with its assumed theoretical construct, while discriminant validity is shown when each measurement item

correlates weakly with all other constructs except for the one to which it is theoretically associated (Geffen & Straub, 2005). Convergent validity measures how the measurement items converge to a latent variable. Convergent validity is calculated by the non-square root AVE scores at the acceptable level of 0.5 or higher (Bagozzi & Yi, 1988). According to Malhotra et al. (2004), establishing convergent validity requires a standardized factor loading that is greater than 0.70 for all latent variables, AVE greater than 0.60, and CR greater than 0.70.

3.5 Structural Model

Once the measurement model has been determined to demonstrate acceptable levels of reliability and validity, the next step is to assess the structural paths of the model as a test of this study's suggested hypotheses. When using PLS-SEM, the coefficient of determination (R^2) is the criterion for assessing the dependent variables in the SEM model and one can interpret them in the same manner as with regression (Chin, 1998).

To test the individual hypotheses, the significance of the t -values reported for the standardized path coefficients calculated by SmartPLS are examined. The significance of the t -values are assessed using a one-tail test because the hypotheses are directional in nature. Figure 3 depicts the PLS hypothesized paths of the structural model.

3.6 Common Method Variance

A prevalent threat to construct validity is common method variance (CMV). Common method variance is defined as the overlap in variance between two variables attributed to the type of measurement instrument (e.g., survey-based) used rather than due to a relationship between the underlying constructs (Avolio et al., 1991). As with all self-reported data, there is a potential for common method bias (CMB) resulting from multiple sources, such as consistency motif and social desirability (Podsakoff et al., 2003; Podsakoff and Organ, 1986).

According to Burton-Jones (2009), CMV is a well-known challenge linked to survey-based quantitative studies resulting from the same respondent providing responses to both exogenous and endogenous construct indicators. Extreme CMV can contribute to CMB resulting in unreliable results. Common method bias happens when variations in responses are caused by the instrument rather than the actual predispositions of the respondents that the instrument attempts to uncover. In other words, the instrument introduces a bias, hence variances, which are analyzed. Consequently, the results are contaminated by the 'noise' stemming from the biased instruments. Researchers have suggested that outcome constructs should have their indicators collected from diverse respondents or at different times than independent constructs (Podsakoff et al., 2012). Podsakoff suggests testing for CMB using Harman's single-factor test, where an unrotated factor solution is checked to see how much variance is explained by a single factor.

According to Williams et al. (1989), evidence of common method bias can be obtained by examining the statistical significance of factor loadings of the method factor and comparing the variances of each observed indicator explained by its substantive construct and the method factor. Additionally, they suggested that the squared values of the method factor loadings were interpreted as the percent of indicator variance caused by method, while the squared loadings of substantive constructs were interpreted as the percent of indicator variance caused by substantive constructs. If the method factor loadings are insignificant and the indicators' substantive variances are substantially greater than their method variances, it can be concluded that common method bias is unlikely to be a serious concern for this study.

3.7 Summary

This chapter addressed the research method approach for this study. The theoretical framework contains the analysis of the underlying principles inherent in attribution theory and the

construction of the relationship between personality and cyber-criminal behaviors. This research approach covers the research design, survey sample and instrument development, data collection, data analysis. The survey sample section contains an approach to the data collection process for sampling and effectiveness. The measurement model discussed the rationale for a quantitative survey research and the study constructs. The instrument development of the constructs presented the logical reasoning behind the adaptation of endogenous and exogenous constructs and the creation of a new instrument. This study also proposed a pathway in testing the reliability and the construct validity of the measurement model. Finally, the structural model tests the structural paths of the model using PLS-SEM.

Chapter 4

Results

4.1 Introduction

Presented in this chapter are presentation and interpretation of the data gathered from the research instruments used in this study. The data gathered in this investigation are arranged based on the presentation of the research question, conceptual and theoretical framework, and hypotheses.

The first section provides an overview of the demographics of the respondents using Statistical Package for Social Sciences (SPSS), followed by a description of the analyses and the findings produced from the analyses. Like other SEM analysis techniques, the overall assessment of the research model takes place in two distinct steps (Hair et al., 2017; Anderson & Gerbing, 1988). First, the measurement model is assessed to assess construct validity. Reflective constructs were assessed for internal consistency and convergent and discriminant validity. The measurement model also was assessed for common method bias. The second step, structural model assessment, tests the strength of the hypothesized relationships between the latent variables in the model (Anderson & Gerbing, 1988). As an added benefit, a zero-order correlation analysis was conducted to determine construct correlation. This chapter concludes with a summary of the findings. Based on these analyses the results of the hypotheses of the study are reported. The quantitative results of the study were generated using SmartPLS version 3.0 (Ringle et al., 2015).

4.2 Descriptive Statistics

Of the original 314 respondents who answered the survey, only 235 respondents were included in the final analysis (79 incomplete responses were received). Table 2 presents a summary

of the demographic characteristics of this sample, including the frequency and percentage of the participants' hacking experience, gender, and age. As shown in Table 2, the majority of respondents in this study were non-hackers (noncombatant; $n = 146$, 62.1%). A slight majority of the participants were men ($n = 130$, 55.3%), and the largest proportion of participants ($n = 68$, 28.9%) was comprised of young adults, ranging in age from 25 to 34 years old.

Table 2: *Descriptive Characteristics of the Full Sample*

Demographic Characteristic	Frequency	Percent
Hacking Experience		
Combatant (0)	89	37.9
Noncombatant (1)	146	62.1
Gender		
Male	130	55.3
Female	105	44.7
Age in years		
18 - 24	61	26.0
25 - 34	68	28.9
35 - 44	52	22.1
45 - 54	49	20.9
55 - 64	4	1.7
65 or older	1	0.4

4.3 Data Analysis

Data analysis was performed using partial least squares (PLS), a variance-based structural equation modelling (SEM) approach allowing simultaneous analysis of both measurement model and structural model. PLS has become prominent in fields including marketing (Hair et al., 2017) and information systems (Ringle et al., 2012), and was chosen in this

study over covariance-based SEM given its suitability for exploration (as is the case here). To address the aims of the study, two PLS models were constructed and analyzed.

The first PLS model (see Figure 4) was constructed to validate the instrument used to measure cyberstalking (i.e., confirmatory factor analysis) and to test Hypotheses 1-3 shown below.

H₁: There is a positive relationship between narcissism and one or more of the cyber-criminal behaviors.

H₂: There is a positive relationship between Machiavellianism and one or more of the cyber-criminal behaviors.

H₃: There is a positive relationship between psychopathy and one or more of the cyber-criminal behaviors.

This model included three exogenous variables (narcissism, Machiavellianism, and psychopathy) with four indicators each. The model also included four endogenous variables: unethical hacking (22 indicators), cyberbullying (five indicators), cyberstalking (18 indicators initially), and identity theft (one indicator). All latent variables were modeled as reflective. Paths were drawn from each exogenous variable (i.e., the Dark Triad personality traits) to each endogenous variable (i.e., cybercrimes). Bootstrapping was performed to obtain significance levels for each of the hypothesized relationships. Given the exploratory nature of this study, two-tailed statistical significance was set at the alpha level of 0.10 prior to any analyses. To determine the statistical significance of factor loadings and paths, bootstrapping was performed using 1000 bootstrapped samples to produce *t*-values. A critical *t*-value of 1.96 was used to determine statistical significance, which corresponds to a two-tailed significance level of $p < .05$.

4.4 Measurement Model Analysis

In social and behavioral science research, reliability assessment in general can be divided into four indicators, namely test–retest reliability, alternative-form reliability, split-half reliability, and internal consistency reliability. Nevertheless, of test–retest reliability, alternative-form reliability, and split-half reliability, all can be called internal consistency reliability. Cronbach’s alpha (α) internal consistency reliability can adopt the most widely reliability indicators (Fornell & Larcker, 1981). Nunnally & Bernstein (1994) indicated 0.7 to be an acceptable reliability coefficient. In the validity analysis of this study, confirmatory factor analysis of the construct measurement model tested each construct for adequate convergent validity and discriminant validity. Accordingly, it was necessary to see if the measurement parameters (especially factor loadings) were operating in the same way for both groups (i.e., a test of measurement invariance) before any evidence bearing on equality of the structural paths was evaluated (i.e., a test of structural invariance). The following sequence analysis of convergent validity and discriminant validity.

All first-order constructs in the research model are reflective, measurement quality being verified by examining convergent validity, discriminant validity, and internal consistency. The influence of zero-order correlation and common methods bias also was scrutinized.

4.4.1 PLS-SEM Model 1

In this study, Anderson and Gerbing (1988) suggested convergent validity analysis criteria, Bagozzi and Yi (1988) proposed confirmatory factor analysis evaluation criteria, and Gefen, Straub, and Boudreau (2000) goodness-of-fit indicators were used to recommend data to assess. Assess standards included: (a) the factor loadings of the indicators respective fields significant; (b) the composite reliability of various dimensions is higher than 0.6; (c) AVE is higher than 0.5, but

0.4 can be accepted because Fornell and Larcker (1981) state that if AVE is less than 0.5, but composite reliability is higher than 0.6, the convergent validity of the construct is still adequate.

First, a CFA was conducted to determine the final indicators for the cyberstalking measure. Initially, all 18 indicators for cyberstalking were included in the model. The loadings for the 18-indicator factor are presented in Table 3.

4.4.2 Convergent Validity

AVE is used as measure of convergent validity (Fornell & Larcker, 1981). Indicators were examined for factor loadings below 0.50. CYST11 had a loading below 0.50 and was removed from the model. Indicator reliability cross-loadings determined that CYST4 loaded more strongly on identity theft than the cyberstalking construct, and CYST5, CYST8, and CYST9 loaded more strongly on the cyberbullying construct than the cyberstalking construct. Therefore, these indicators also were removed from the model. Finally, a multigroup analysis revealed that CYST1 and CYST10 were perfectly correlated in the noncombatant group, preventing calculation of the multigroup models. Therefore, CYST1 (the lower loading item of the two) was removed from the model. No additional items could be removed to improve the reliability and validity of the cyberstalking construct. The reliability of cyberstalking was high (Cronbach's $\alpha = .91$) and AVE was below .50 (AVE = .46), but acceptable at 0.4. The reliability analysis and convergent validity analysis is obtained.

Table 3: *Factor Loadings for Cyberstalking with 18 Indicators*

Indicator	Loading
CYST1*	0.53
CYST2	0.53
CYST3	0.65
CYST4*	0.52

CYST5	0.63
CYST6	0.81
CYST7	0.81
CYST8*	0.71
CYST9*	0.66
CYST10	0.61
CYST11*	0.49
CYST12	0.60
CYST13	0.65
CYST14	0.82
CYST15	0.61
CYST16	0.62
CYST17	0.73
CYST18	0.60

Note. * Denotes items removed from the model

Further, Cronbach's α values range between 0.76 and 0.96, all of which are higher than the reliability standard 0.7. Not surprisingly, all Dark Triad components, measured on the Dirty Dozen scale, were moderately to highly correlated, supporting the conviction that they share a common core (Paulhus, & Williams, 2002). The "square root" of AVE has been calculated in Table 4 denoted as CR. Each construct's CR is between 0.66 and 0.72, higher than the standard 0.6.

Table 4 presents the final factor loadings, reliability, and validity statistics from the CFA for only those items that were included in the models. All indicator loadings for cyberstalking exceeded 0.50 and all t -values exceeded 1.96, indicating convergent validity, whereby all indicators loaded significantly onto the construct.

4.4.3 Internal Consistency

Internal consistency was assessed via Cronbach's α values, all of which were above 0.7, indicating either excellent (0.91 and above) or high (0.76-0.83) reliability. Although, Cronbach's α is used to measure internal consistency reliability, it tends to provide a conservative measurement in PLS-SEM. Prior literature has suggested the use of composite reliability (CR) as a replacement

(Hair et al. 2014). Internal consistency was assessed by means of composite reliability measures (CR), all of which were well in excess of the 0.6 threshold (Hair et al.2014; Bagozzi and Yi, 1988). High levels of internal consistency reliability have been demonstrated among all reflective latent variables. By using CR scores, such values were shown to be larger than 0.6, proving reliability.

Table 4: *Factor Loadings, Reliability, and Validity Statistics for Study Constructs*

Variable	Cronbach's Alpha (α)	AVE (CR)	Loading	<i>t</i> -value
Cyberbullying	.79	.43 (.66)		
CYBU1			0.73	11.64
CYBU2			0.79	14.06
CYBU3			0.62	8.48
CYBU4			0.58	8.68
CYBU5			0.53	6.33
Cyberstalking	.91	.46 (.68)		
CYST2			0.53	5.23
CYST3			0.65	8.90
CYST6			0.81	10.68
CYST7			0.81	14.29
CYST10			0.61	6.79
CYST12			0.60	7.92
CYST13			0.65	7.57
CYST14			0.81	12.95
CYST15			0.61	6.57
CYST16			0.62	7.78
CYST17			0.73	9.76
CYST18			0.60	7.15
Identity theft	1.00	1.00 (1.00)		
IDTH1			1.00	-
Unethical hacking	.96	.51 (.72)		
UH1			0.66	8.73
UH2			0.72	10.86
UH3			0.58	7.04
UH4			0.63	7.66
UH5			0.47	5.04

UH6			0.38	3.03
UH7			0.25	2.34
UH8			0.81	15.21
UH9			0.87	22.33
UH10			0.75	15.04
UH11			0.80	13.42
UH12			0.69	10.70
UH13			0.68	10.45
UH14			0.83	15.27
UH15			0.85	18.53
UH16			0.81	15.94
UH17			0.71	9.57
UH18			0.81	16.66
UH19			0.82	17.72
UH20			0.83	19.08
UH21			0.87	17.30
UH22			0.54	6.21
<hr/>				
Machiavellianism	.83	.55 (.74)		
MACH1			0.76	16.24
MACH2			0.75	15.06
MACH3			0.61	10.58
MACH4			0.83	15.72
<hr/>				
Narcissism	.79	.49 (.70)		
NARC1			0.71	7.60
NARC2			0.77	9.35
NARC3			0.79	9.53
NARC4			0.49	4.27
<hr/>				
Psychopathy	.76	.43 (.66)		
PSYCH1			0.63	6.86
PSYCH2			0.46	3.62
PSYCH3			0.60	6.92
PSYCH4			0.88	12.45

Note. Composite Reliability (CR) = square root of AVE.

4.4.4 Discriminant Validity Analysis

Previous guidelines for PLS-SEM encouraged using the Fornell-Larcker criterion to evaluate discriminant validity (Hair et al., 2013). The Fornell & Larcker approach is certainly the most common technique for detecting discriminant validity violations on the construct level. An

alternative technique, proposed by Henseler et al. (2015), is the heterotrait–monotrait (HTMT) ratio of correlations. Based on simulation data, these authors show for variance-based SEM; e.g., PLS, that AVE does not reliably detect discriminant validity violations, whereas HTMT identifies a lack of discriminant validity effectively (Hair et al., 2017; Henseler et al., 2015).

There are two ways of using the HTMT to assess discriminant validity: (1) as a criterion or (2) as a statistical test. First, using the HTMT as a criterion involves comparing it to a predefined threshold. If the value of the HTMT is higher than this threshold, one can conclude that there is a lack of discriminant validity. The exact threshold level of the HTMT is debatable among researchers. Some authors suggest a threshold of 0.85 (Clark & Watson, 1995; Kline, 2011), whereas others propose a value of 0.90 (Gold et al., 2001; Teo et al., 2008). The HTMT is an estimate for the factor correlation (more precisely, an upper boundary).

In a recent study using inferential tests, it was determined that the HTMT ratio between any two reflective constructs should not exceed 1.0 (Henseler et al., 2016). Further, Franke and Sarstedt (2018) determined that $HTMT_1$ have the highest threshold for inferring a lack of discriminant validity and therefore should produce the fewest errors when the construct correlation (ϕ_{XY}) actually is less than 1. $HTMT_{.90}$ and $HTMT_{.85}$ may signal that two constructs lack discriminant validity when ϕ_{XY} is very high, say .95, but actually less than 1.

The HTMT ratios between each reflective construct are shown in Table 5 below. All of the ratios are less than 0.85, 0.90 and 1.0. The ratio between unethical hacking and cyberbullying, at 0.990, shows these two constructs are closely related. From the HTMT results in Table 5, the values indicate no discriminant validity problems according to the $HTMT_1$ criterion.

Table 5: Heterotrait–Monotrait (HTMT) Results

	CB	CS	IT	MACH	NARC	PSYCH
CB						
CS	0.803					
IT	0.581	0.552				
MACH	0.728	0.686	0.280			
NARC	0.411	0.432	0.251	0.736		
PSYCH	0.503	0.465	0.203	0.740	0.553	
UH	0.990	0.767	0.482	0.701	0.413	0.567

Note. 1 / 0.90 / 0.85 > HTMT

Discriminant validity also was evaluated through cross-loadings of the cyberstalking indicators with the other constructs and through construct correlations (see Table 6). All cyberstalking indicators loaded most strongly on the cyberstalking construct. The correlations between cyberstalking and identity theft, narcissism, and psychopathy were lower than the square root of cyberstalking's AVE (0.67), but the correlations between cyberstalking and cyberbullying, unethical hacking, and Machiavellianism were higher than the square root of cyberstalking's AVE.

Table 6: Cyberstalking Indicator Cross-Loadings and Construct Correlations

Indicator	CS	CB	IT	UH	MACH	NARC	PSYCH
CYST2	0.53	0.27	0.24	0.31	-0.36	-0.23	-0.30
CYST3	0.65	0.55	0.39	0.51	-0.45	-0.31	-0.28
CYST6	0.81	0.66	0.27	0.65	-0.56	-0.27	-0.37
CYST7	0.81	0.69	0.49	0.65	-0.56	-0.29	-0.41
CYST10	0.61	0.55	0.36	0.49	-0.42	-0.33	-0.32
CYST12	0.60	0.52	0.51	0.51	-0.42	-0.34	-0.29
CYST13	0.65	0.53	0.28	0.50	-0.45	-0.30	-0.33
CYST14	0.81	0.54	0.26	0.57	-0.56	-0.36	-0.42
CYST15	0.61	0.58	0.53	0.46	-0.43	-0.30	-0.26
CYST16	0.62	0.48	0.34	0.41	-0.43	-0.21	-0.31
CYST17	0.73	0.56	0.36	0.49	-0.51	-0.25	-0.32
CYST18	0.60	0.52	0.45	0.47	-0.42	-0.30	-0.29
Correlations with Cyberstalking	-	0.79	0.55	0.74	-0.69	-0.43	-0.48

Notes. CS = cyberstalking. CB = cyberbullying. IT = identity theft. UH = unethical hacking. MACH = Machiavellianism. NARC = narcissism. PSYCH = psychopathy.

4.4.5 Zero-Order Correlation

The data was analyzed using a zero-order correlation to determine if any of the cybercriminal behaviors were significantly related to any of the Dark Triad factors being measured. Logistic regression was used to measure the variables significantly related to each behavior according to the zero-order correlation, as it is a robust measure and appropriate for exploratory analysis (Field, 2009). All zero-order correlations between the study constructs are presented in Table 7.

There were statistically significant zero-order positive correlations between all cybercriminal behaviors. As seen in Table 7, unethical hacking behavior was significantly related to cyberstalking behavior ($r = 0.75, p < .001$), cyberbullying behavior ($r = 0.99, p < 0.001$), and identity theft behavior ($r = 0.45, p < 0.001$). Cyberbullying behavior was significantly related to cyberstalking behavior ($r = 0.80, p < 0.001$). Identity theft behavior was significantly related to cyberstalking ($r = 0.54, p < 0.001$) and cyberbullying ($r = 0.56, p < 0.001$) behaviors. Of the Dark Triad traits, narcissism significantly related to Machiavellism ($r = 0.71, p < 0.001$). Psychopathy was significantly related to Machiavellianism ($r = 0.75, p < 0.001$) and narcissism ($r = 0.53, p < 0.001$). Finally, there were no zero-order positive correlations between the Dark Triad and cybercriminal behaviors.

Table 7: Zero-Order Correlations Between Study Constructs

Variable	CS	CB	IT	UH	MACH	NARC
CS	-					
CB	0.80 †	-				
IT	0.54 †	0.56 †	-			
UH	0.75 †	0.99 †	0.44 †	-		
MACH	-0.69	-0.73	-0.28	-0.71**	-	
NARC	-0.43	-0.41	-0.25	-0.40	0.71 †	-
PSYCH	-0.48	-0.53	-0.20	-0.60	0.75 †	0.53 †

* $p < 0.05$, two-tailed. ** $p < 0.01$, two-tailed. † $p < 0.001$, two-tailed.

Notes. CS = cyberstalking. CB = cyberbullying. IT = identity theft. UH = unethical hacking. MACH = Machiavellianism. NARC = narcissism. PSYCH = psychopathy.

Note. $N = 235$

4.4.6 Common Method Bias

Common methods bias (CMB) can be a major source of measurement error for survey-based research (Bagozzi and Yi, 1988). Given that high CMB may lead to incorrect conclusions being reached about relationships between constructs, Harman's single-factor test (Podsakoff et al., 2003) was used to check if a single common factor accounted for the majority of variance across all factors (see Table 8). According to Podsakoff and Organ (1986), there is evidence for common method bias if the 1-factor solution explains 50% or more of the variance in the data. The Harman's test yielded a single factor accounting for 38.15% of total variance, suggesting that CMB was not present in the data.

Table 8: Harman's Single-Factor Test

Component	Total	% of Variance	Cumulative %
1	19.840	38.154	38.154

Results from evaluation of the measurement model therefore demonstrated the adequate convergent and discriminant validity, internal consistency, and absence of CMB necessary to justify testing of the hypotheses.

With the completion of reliability and validity testing in PLS-SEM Model 1 (measurement model), next is the path analysis for the PLS-SEM model 1 for coefficient testing and prediction in the structural model analysis.

4.5 Structural Model Analysis

In PLS-Model 1, analysis of whether the path coefficients are significant to the study hypotheses 1-3 are tested. So, in order to estimate whether the path coefficients are significant, Hair et al. (2013) recommend using bootstrap method. That is, the use of the t -value to estimate the p -value, to test the significance of coefficient, and to determine whether the hypothesis was supported. The predictive power of the model is determined by the use of R -squared (R^2). Results of hypothesis testing are summarized in Figure 4.

The path coefficients showing the relationships between the Dark Triad personality traits and the cybercrime measures are displayed in Table 9. R^2 values for the cybercrime measures were 0.55, 0.49, 0.09, and 0.53 for cyberbullying, cyberstalking, identity theft, and unethical hacking, respectively. The larger the value, the better is the explanatory power of the model. In general, R^2 value greater than 0.67 is a practical value, the R^2 value represents a moderate explanatory power between 0.33 and 0.66, and R -squared value between 0.19 and 0.32 is weak explanatory power (Chin et al., 2003). Therefore, the model showed weak to moderate explanatory power.

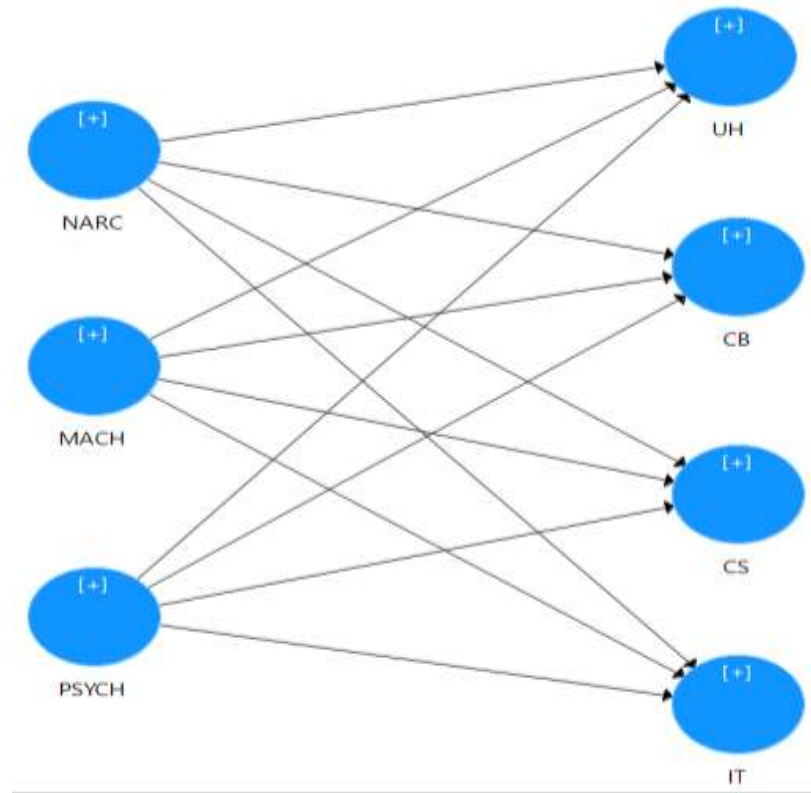


Figure 4. *Structural PLS-SEM Model 1*

Table 9: *Path Coefficients for PLS-SEM Model 1*

Path	Overall		Combatant		Noncombatant		<i>t</i> Difference
	β	<i>t</i>	β	<i>t</i>	β	<i>t</i>	
MACH -> CB	-0.91	4.42	-0.44	3.98	-0.52	4.34	0.47
MACH -> CS	-0.84	4.09	-0.57	5.43	-0.36	2.59	1.10
MACH -> IT	-0.23	1.15	-0.11	1.02	-0.26	1.54	0.64
MACH -> UH	-0.73	4.37	-0.48	4.71	-0.35	3.23	0.85
NARC -> CB	0.21	1.56	-0.11	1.09	0.15	1.14	1.39
NARC -> CS	0.13	1.01	-0.07	0.59	-0.07	0.51	0.02
NARC -> IT	-0.11	0.84	-0.22	2.44	0.09	0.55	1.38
NARC -> UH	0.19	1.69	-0.10	0.98	0.01	0.06	0.59
PSYCH -> CB	0.04	0.23	-0.03	0.34	-0.08	0.71	0.28
PSYCH -> CS	0.08	0.45	0.03	0.30	-0.12	1.02	0.89
PSYCH -> IT	0.03	0.16	0.06	0.39	-0.20	1.73	1.38
PSYCH -> UH	-0.16	1.10	-0.11	1.16	-0.15	1.55	0.29

Notes. CS = cyberstalking. CB = cyberbullying. IT = identity theft. UH = unethical hacking. MACH = Machiavellianism. NARC = narcissism. PSYCH = psychopathy.

4.5.1 Hypothesis Results

H₁: There is a positive relationship between narcissism and one or more of the cyber-criminal behaviors.

Hypothesis 1 was not corroborated by the results in Table 9, such that no path coefficients for narcissism were significant, indicating that narcissism was not significantly related to the cybercrime measures.

H₂: There is a positive relationship between Machiavellianism and one or more of the cyber-criminal behaviors.

Hypothesis 2, which predicted a positive relationship between Machiavellianism and these measures, was not supported by the findings. Specifically, the results showed significant negative path coefficients from Machiavellianism to cyberbullying ($\beta = -0.91, t = 4.42, p < 0.05$), cyberstalking ($\beta = -0.84, t = 4.09, p < 0.05$), and unethical hacking ($\beta = -0.73, t = 4.37, p < 0.05$), indicating that Machiavellianism was significantly negatively related to these cybercrime measures.

H₃: There is a positive relationship between psychopathy and one or more of the cyber-criminal behaviors.

Contrary to expectations, Hypothesis 3 was not confirmed based on the findings shown in Table 9. Psychopathy was significantly negatively related to these cybercrime measures, whereby no path coefficients for psychopathy were significant. As Hypothesis 3 predicted a positive relationship between psychopathy and these cybercrime measures, Hypothesis 3 was not supported.

Finally, a multigroup analysis showed that there were no significant differences in the path coefficients between the combatant and noncombatant participants (see *t* Difference column in

Table 9). Taken together, the results from the structural PLS-SEM Model 1 did not provide support for Hypotheses 1-3.

4.6 Post-Hoc Analysis

As a post-hoc analysis, correlation of Dark Triad and criminal behaviors in terms of gender differences (Hypothesis 4) and/or age (Hypothesis 5) was assessed. This PLS-SEM model hypothesizes age (AGE) and gender (GENDER) are potential moderators of the relationship between DT traits and cyber-criminal behaviors. Therefore, the second PLS-SEM Model 2 (see Figure 5) was constructed as a post-hoc analysis to address Hypotheses 4 and 5 shown below.

H4: The relationship between Dark Triad variables and cyber-criminal behaviors would be significantly higher in males than females.

H5: The relationship between Dark Triad variables and cyber-criminal behaviors would be portrayed in higher levels among younger adults than in older adults.

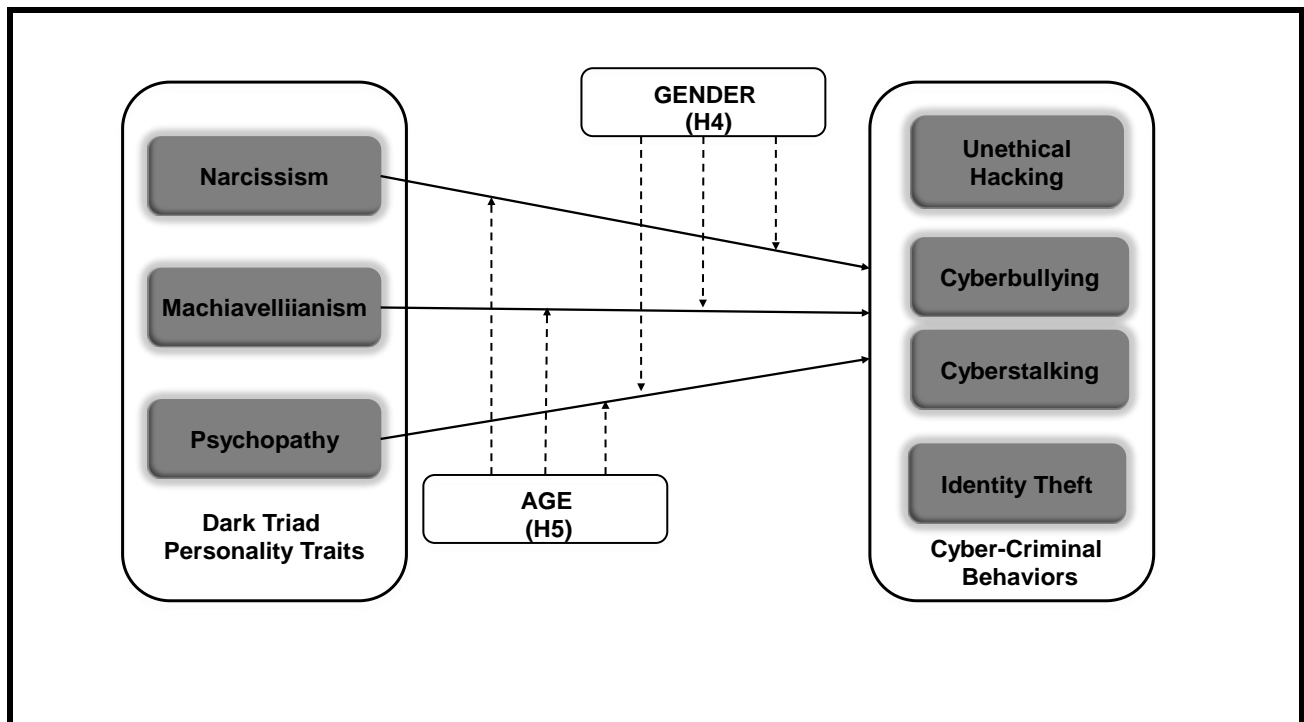


Figure 5: Concept of Structural PLS-SEM Model 2

This model was constructed in the same way as the PLS-SEM Model 1 with gender and age added as moderating variables. Paths were drawn from gender and age to each endogenous variable, and interaction terms were computed to determine the moderating effect of gender and age on the relationship between each exogenous variable and each endogenous variable. An accurate visual depiction of the PLS-SEM Model 2 was not legible to place within this paper. Therefore, shown below illustrates the paths that were drawn within SmartPLS for the structural model.

❖ Paths drawn:

- Narcissism, Machiavellianism, psychopathy, gender, and age to unethical hacking
- Narcissism, Machiavellianism, psychopathy, gender, and age to cyberbullying
- Narcissism, Machiavellianism, psychopathy, gender, and age to cyberstalking
- Narcissism, Machiavellianism, psychopathy, gender, and age to identity theft

❖ Moderating effects applied to each dependent variable:

- Narcissism x gender
- Narcissism x age
- Machiavellianism x gender
- Machiavellianism x age
- Psychopathy x gender
- Psychopathy x age

A moderator is a variable that specifies conditions under which a given predictor is related to an outcome. The moderator explains when a dependent variable (DV) and independent variable (IV) are related (Aiken & West, 1991). In hypotheses, H4 and H5 (see Figure 6) moderating variables are to check the moderating effect on IV (DT) and DV (CB) relation.

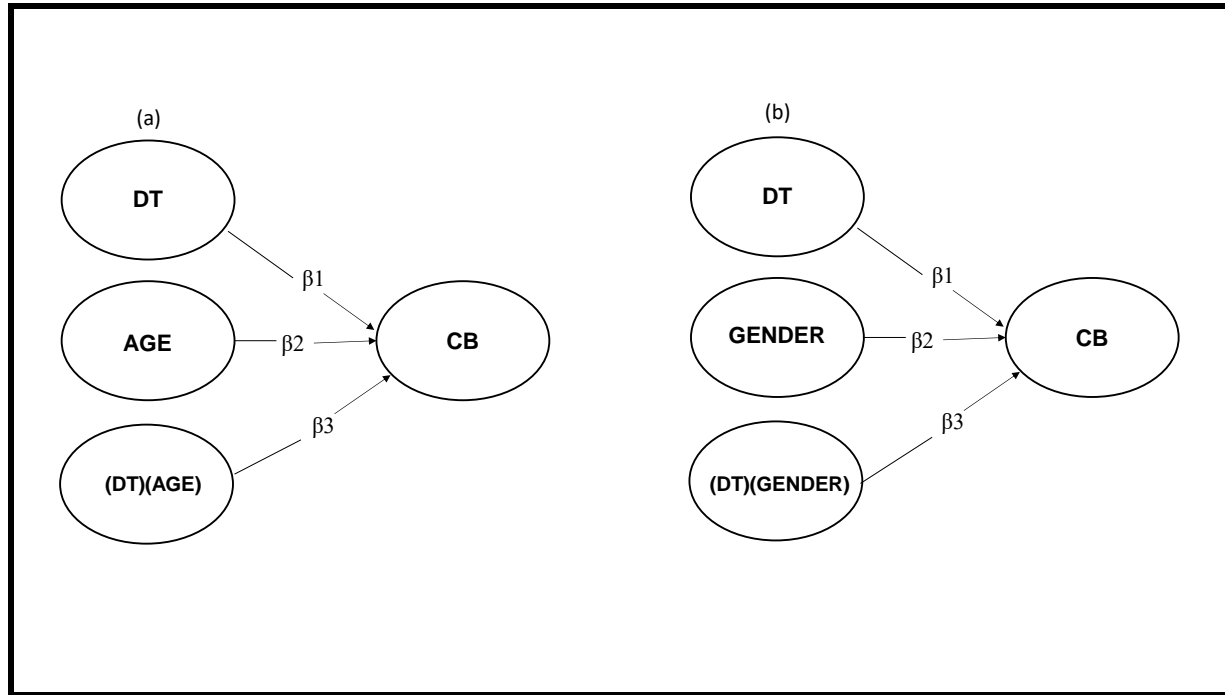


Figure 6: Moderating Variable Assessment

The DT is the independent variable, while CB is the dependent variable. In Figure 6a, β_1 is the effect of independent variable DT on dependent variable CB, β_2 is the effect of the moderator variable AGE on the CB, and β_3 is the effect of the product of DT and AGE on CB. In Figure 6b, β_1 is the effect of DT on CB, β_2 is the effect of the GENDER on the CB, and β_3 is the effect of the product of GENDER and DT on CB. Notably, the one-way arrow is indicative of the direction of impact from one variable to another; as such, it is the structural regression coefficient (Byrne, 2013).

Following Awang (2012, p. 131), the study will evaluate the moderating effect of AGE by using Equation 1 for Figure 6a and Equation 2 for Figure 6b.

Equation 1:

$$CB = \beta_0 + \beta_1 DT + \beta_2 AGE + \beta_3 (DT)(AGE) + e$$

Equation 2:

$$CB = \beta_0 + \beta_1 DT + \beta_2 GENDER + \beta_3 (DT)(GENDER) + e$$

The intercept of the equation is β_0 , the residual is e , the coefficient of DT to CB when AGE is zero is β_1 , and the coefficient of AGE to CB when DT is zero is β_2 . Henceforth, the regression coefficient of β_3 will provide an estimated moderation of the interaction. The test for interaction effect in this study is consistent with the literature, which requires a causal theory and design behind the data for estimation of causal interaction effect (Awang, 2012). A statistically significant β_3 from zero will indicate there is a significant moderation of DT to CB in the data.

4.6.1 PLS-SEM Model 2 - Moderating Variables

The path coefficients added to PLS-SEM Model 2 (i.e., gender, age, and their moderating effects) are displayed in Table 10. R^2 values for the cybercriminal measures were 0.65, 0.59, 0.20, and 0.64 for cyberbullying, cyberstalking, identity theft, and unethical hacking respectively. The moderating effect of age on the relationship between narcissism and identity theft was significant ($\beta = 0.33$, $t = 2.45$, $p < 0.05$), indicating that as age increased, the relationship between narcissism and identity theft became stronger. Hypotheses 4 predicted a relationship between Dark Triad variables and criminal behaviors would be significantly higher in males than females. Therefore, the expectation that more males would be computer deviants than females was not supported. Hypothesis 5 was not supported, which predicted criminal behaviors would be portrayed in higher levels among younger adults than in older adults.

A multigroup analysis showed that there was a positive significance in the moderating path of age on cyberstalking ($t = 1.99$, $p < 0.05$). There were no other significant differences in the moderating path coefficients between the combatant and noncombatant participants (see t Difference column in Table 10).

Table 10: *Path Coefficients for PLS-SEM Model 2*

Path	Overall		Combatant		Noncombatant		<i>t</i> Difference
	β	<i>t</i>	β	<i>t</i>	β	<i>t</i>	
Age -> CB	-0.21	0.17	-0.18	1.37	-0.06	0.53	0.70
Age -> CS	-0.11	0.10	0.16	1.13	-0.20	1.78	1.99
Age -> IT	-0.13	0.26	-0.08	0.45	-0.13	1.14	0.26
Age -> UH	-0.18	0.26	-0.16	1.16	-0.14	1.06	0.10
Gender -> CB	-0.28	0.10	-0.25	1.96	-0.10	1.05	0.89
Gender -> CS	-0.18	0.09	-0.16	1.17	-0.16	1.62	0.00
Gender -> IT	-0.16	0.23	-0.08	1.00	-0.16	1.76	0.59
Gender -> UH	-0.34	0.22	-0.30	1.87	-0.20	2.34	0.61
Age*MACH -> CB	0.08	0.04	0.09	0.69	0.01	0.05	0.39
Age*NARC -> CB	0.05	0.10	-0.11	0.82	0.10	0.73	1.04
Age*PSYCH -> CB	0.11	0.03	0.09	0.62	0.17	1.22	0.40
Gender*MACH -> CB	0.19	0.08	0.00	0.02	0.34	2.24	1.55
Gender*NARC -> CB	-0.05	0.08	-0.07	0.85	-0.15	0.98	0.38
Gender*PSYCH -> CB	0.20	0.05	0.17	1.13	0.13	1.14	0.21
Age*MACH -> CS	0.02	0.01	0.01	0.04	0.08	0.66	0.34
Age*NARC -> CS	0.13	0.45	-0.18	0.97	0.21	1.42	1.65
Age*PSYCH -> CS	0.06	0.02	0.14	0.82	0.26	1.66	0.51
Gender*MACH -> CS	0.19	0.12	0.05	0.34	0.23	1.56	0.81
Gender*NARC -> CS	0.05	0.09	0.03	0.32	0.02	0.10	0.07
Gender*PSYCH -> CS	0.17	0.06	0.21	1.26	0.24	1.98	0.15
Age*MACH -> IT	-0.23	0.35	-0.15	0.92	-0.12	0.83	0.12
Age*NARC -> IT	0.33	2.45	0.24	1.05	0.25	1.46	0.02
Age*PSYCH -> IT	0.11	0.09	-0.02	0.09	0.20	1.23	0.80
Gender*MACH -> IT	0.02	0.05	-0.02	0.17	0.23	1.36	1.07
Gender*NARC -> IT	0.24	1.20	0.12	1.49	0.07	0.35	0.20
Gender*PSYCH -> IT	0.01	0.01	-0.01	0.09	0.02	0.16	0.17
Age*MACH -> UH	0.09	0.07	0.00	0.03	-0.01	0.10	0.09
Age*NARC -> UH	0.05	0.14	-0.05	0.38	0.21	1.33	1.15
Age*PSYCH -> UH	0.05	0.03	0.10	0.74	0.23	1.26	0.49
Gender*MACH -> UH	0.19	0.11	-0.01	0.04	0.23	1.52	1.05
Gender*NARC -> UH	-0.04	0.09	-0.02	0.20	0.06	0.30	0.31
Gender*PSYCH -> UH	0.18	0.09	0.24	1.29	0.16	1.27	0.39

Notes. CS = cyberstalking. CB = cyberbullying. IT = identity theft. UH = unethical hacking. MACH = Machiavellianism. NARC = narcissism. PSYCH = psychopathy.

Second-Order Analysis of PLS-SEM Models

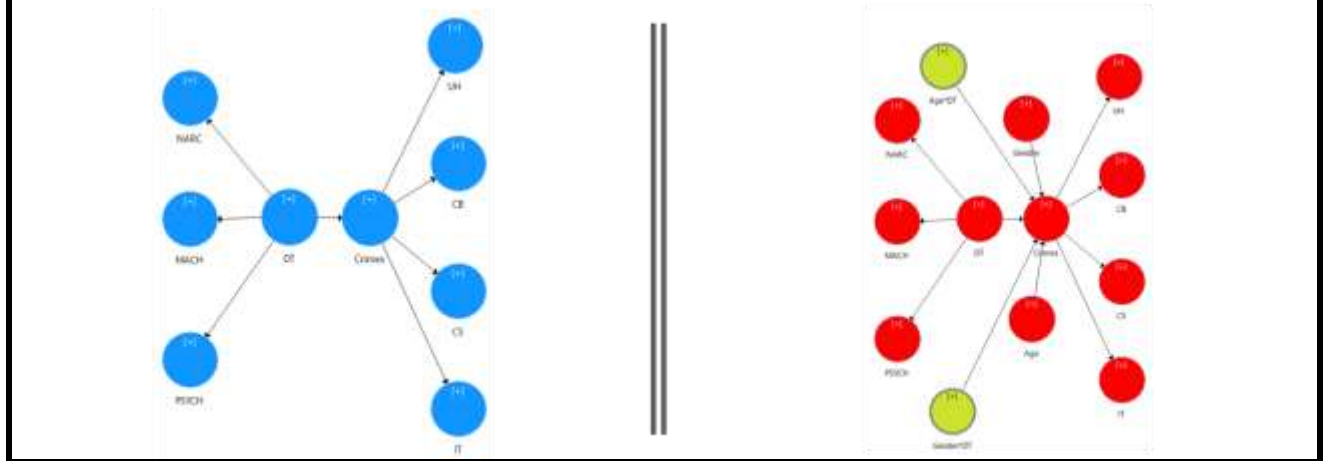


Figure 7. *Structural PLS-SEM Models 1&2 with Second Order*

4.6.2 Second-Order Analysis of PLS-SEM Models

The previous PLS models (1 and 2) were replicated with the Dark Triad (DT) and cybercrimes treated as single second-order constructs (see Figure 7). The results of the second-order models are presented in Table 11. The Dark Triad was significantly negatively related to cybercrimes ($\beta = -0.67$, $t = 14.26$, $p < 0.05$). Gender significantly moderated the relationship between Dark Triad and cybercrimes ($\beta = 0.27$, $t = 5.61$, $p < 0.05$), indicating that the negative relationship between Dark Triad and cybercrimes was stronger for women compared to men. A multigroup analysis showed that there were no significant differences in the path coefficients between the combatant and noncombatant participants (see t Difference column in Table 11).

Table 11: *Path Coefficients for Second Order PLS-SEM Models*

	Overall		Combatant		Noncombatant		
Path	β	t	β	t	β	t	t Difference
Model 1							
DT -> Crimes	-0.67	14.26	-0.58	9.25	-0.42	3.48	0.98
Model 2 (Added Paths)							
Age -> Crimes	-0.12	1.80	-0.10	0.78	-0.09	1.13	0.04
Gender -> Crimes	-0.29	5.82	-0.21	1.94	-0.15	2.08	0.44
Age*DT -> Crimes	0.13	1.79	0.04	0.45	0.31	2.14	1.37
Gender*DT -> Crimes	0.27	5.61	0.13	0.93	0.34	2.67	1.10

Notes. DT = Dark Triad.

4.7 Summary

Two PLS models were constructed to address the research question and hypotheses of the study. The results of PLS-SEM Model 1 showed that there were no positive relationships between the Dark Triad personality traits and the cybercriminal measures; however, Machiavellianism was significantly negatively related to cyberbullying, cyberstalking, and unethical hacking. Hypotheses 1-3 were not supported. The results of the PLS-SEM Model 2 showed that age moderated the relationship between narcissism and identity theft such that as age increased, the relationship between narcissism and identity theft became stronger. The expectation that more males would be computer deviants than females was not supported. Combatants and noncombatants were all found to have no significant path coefficients. A second-order analysis indicated that the negative relationship between Dark Triad and cybercrimes was stronger for women compared to men. The next chapter contains a discussion of these findings in relation to previous literature, as well as recommendations for future research.

CHAPTER 5

Conclusions, Implications, Recommendations, and Summary

5.1 Discussion

Despite the increasing evidence justifying the effects of the Dark Triad traits on various deviant behaviors, scant attention has been given to the underlying mechanism and processes through which this relationship occurs. Therefore, the purpose of this study is to explore the psychological mechanism that underlies the association between the Dark Triad traits and cybercriminal behaviors.

By applying the dispositional elements of the attribution theory, the relations between the Dark Triad and cybercriminal behaviors (including unethical hacking, identity theft, cyberbullying, and cyberstalking) were tested. According to this theory, the personality traits of an individual determines their behavior (Heider, 1958). The current study was the first to compare computer deviancy against the Dark Triad using the attribution theory. Scholars in the psychology, criminology, and information systems fields have suggested the Dark Triad personality traits were related to criminal or deviant behavior (Nevin, 2015; Maasberg et al., 2015; Goodboy & Martin, 2015).

The study aimed to assess the prevalence of cybercriminal behavior and which personality factors were related to each specific type of defined cybercriminal behaviors. The current study found that 62.1% of the respondents (n = 146) included in the final analysis were categorized as non-combatants. Although there were 37.9% of participants categorized as combatants, the total number of combatants that attempted the survey (n = 149) outweighed that of combatants. The demographic showed that there were more participant males (55.3%) than females (44.7%). This finding is consistent with prior research (Loper, 2000; Parker, 1998; Rogers, 1999:2006).

In this study, two groups of individuals were recruited, combatants (hackers) and non-combatants (non-hackers). To address the research question of the present study, a survey measurement instrument (see Appendix A) was developed and fielded at the Black Hat, DefCon, and BSides hacker conventions in Las Vegas (see Appendix C). These conventions have developed into some of the largest and most popular annual conventions worldwide. The convention is attended by a diverse audience comprised of American and international hackers and security experts (Coleman, 2010). Additional survey scores were collected via other security conferences and a general population of social media users (non-hackers).

The survey instrument included a newly devised scale for cyberstalking, which was appended to the existing validated CCI-R+ scale (Seigfried-Spellar et al., 2015; Seigfried-Spellar & Treadway, 2014). The CCI-R+ examines computer deviant characteristics among respondents who admitted to having engaged in illicit hacking activities and assesses the relevance of hacking-related outcomes. The cyberstalking construct was tested for validity and reliability and assessed the ability to cleanly measure via CFA.

The current study found that each computer deviant behavior was significantly related to all other computer deviant behaviors. Which was consistent with prior findings (Seigfried-Spellar et al., 2015:2017; Loper, 2000; Parker, 1998; Rogers, 1999:2006). Internal consistency among the CCI-R+ (with cyberstalking included) was proven. The Dark Triad traits were measured with the Dirty Dozen scale (Jonason, & Webster, 2010). Fortunately, existing research suggests that these measures typically have desirable psychometric properties, including relatively high levels of reliability and convergent, discriminant, and construct validity. All three four-item subscales of the Dirty Dozen were internally consistent: narcissism ($\alpha=.79$), psychopathy ($\alpha=.76$), and Machiavellianism ($\alpha=0.83$). This is consistent with previous research (Jonason & Webster, 2010). Some researchers have indicated that all Dark Triad personality traits had a significantly positive

relationship with cyberbullying (Hajlo et al., 2015; Goodboy & Martin, 2015). Psychopathy has been tied to unethical hacking behaviors (Nevin, 2015). Also, Machiavellianism and psychopath personality traits were respectively the strongest variables in predicting cyberbullying. Harrison, Summers, and Mennecke (2016) assert that individuals rating high in the Machiavellian trait are more likely to commit fraud (e.g., identity theft) and lie to, steal from, cheat, and mislead others. Given that Dark Triad traits associate with values such as power, hedonism, and manipulation (Jones & Figueredo, 2013; Kajonius et al., 2015), individuals high on the aforementioned traits may engage in cyberstalking. Moreover, women higher in narcissism want the upper hand in their relationship by following online interactions of their intimate partners by engaging in cyberstalking behavior (Smoker & March, 2017). Given the aforementioned research, surprisingly, none of the computer deviant behavior specific hypotheses were supported.

It should be pointed out that the conclusions are based on the PLS-SEM Model 1 that we examined with each of the three Dark Triad traits as an independent variable, and cyber-criminal behaviors as a dependent variable. Although, the results did not support the causal processes proposed in the hypothesis development sections, this study also tested the competing PLS-SEM Model 2. Additionally, the validity and reliability of the constructs, provides further research into possibly adding the cyberstalking category to the CCI-R+ instrument.

As an ad hoc analysis, the moderator variables (age and gender) between the Dark Triad of personality and cybercrimes also were investigated in PLS-SEM Model 2. The results of the model showed that age moderated the relationship between narcissism and identity theft such that as age increased, the relationship between narcissism and identity theft became stronger. The expectation that more males would participate in cybercriminal behavior than females was not supported, but according to previous research males are more likely to be hackers compared to females (Spertus, 1991; Turkle, 2005). As such, it was necessary to examine the gendered experiences of hackers to

consider why this disparity exists, and how male dominated organizational structure affects hacker subculture, as well as any differences in male and female hackers (Turkle, 1984). Such research also could establish any links between the skills of female hackers and those of the larger population of female deviants or criminals.

5.2 Implications

Our research brings significant theoretical implications for the literature on cybercriminal behaviors within SNSs. To our knowledge, this study is among the first attempts to examine the impact of the Dark Triad traits on cybercriminal behaviors applying the attribution theory. Firstly, this study extends the preliminary research on criminality from the perspective of individual differences, but does not confirm the relationship between each Dark Triad trait and certain cybercriminal categories. Rampant threats to SNSs have raised questions surrounding the personality traits responsible for these threats. In other words, do the Dark Triad personality traits facilitate criminal behavior? To a certain extent, the current study seems to have answered this question by revealing that the Dark Triad and cybercriminal factors had high Cronbach's alpha scores, showing internal consistency of the constructs.

There have been several theories over the years used to examine the motivations behind deviant or criminal behaviors. Exploring hacker subcultures, Williams (2006) suggested it was futile to attempt to provide a universal theory of cybercrime. Thus, secondly, the present study furthered the research on the attribution theory, and encourages researchers to understand the occurrence of computer deviancy by providing insight into the underlying psychological mechanisms between the Dark Triad of personality and cyber-criminality. Thirdly, these findings also enrich the studies on the attribution theory and establish that people's motivations to commit deviant acts are not independent of outcome and more future research is warranted.

Although analysis did not support the hypothetical outcomes, it is noteworthy that this study was pragmatic because it provided some good measures. Moreover, moderating roles of age and gender was unable to support the reason why the Dark Triad traits facilitate cyber-criminality. Finally, at the individual level, although one's personality cannot be easily changed, if individuals could become aware that their personality predisposes them to engage in deviant behaviors, then they could take more positive steps to deter them. Overall, this study offers an original take on personality traits and their potential in cybercriminals. Due to the relatively small sample sizes available, and the different gender ratios in our two groups (combatants vs. non-combatants), it offers seed evidence to guide future research.

5.3 Limitations

There is no doubt that this study has several limitations. First of all, the cross-sectional data and correlational design does not allow us to detect the causal link between the Dark Triad of personality and cybercriminal behaviors. Longitudinal studies should be conducted to replicate these findings in future. Second, it is also important to note that although self-report measures are widely used and the instruments employed in present study have good reliability and validity, a response bias is inevitable. For example, survey scores were taken from two groups of participants: combatants and non-combatants. Whether or not people are honest when answering questions as part of a survey is a thread that is woven through past methodological work on survey research. Participation bias also can be a problem, occurring when a certain group of participants are more or less likely to participate than others. This can happen when a certain group appreciates the value of surveys more than others (combatants vs. non-combatants) or if survey takers are incentivized, such as by cash payment. Compensating survey participants is a very contentious practice and usually will result in people taking the survey who are not in the intended sample population.

Thirdly, connections between the DefCon and the Black Hat computer security conference, as described in Chapter Three, shed light on the increasing legitimization of hacking. The presence of hiring professionals at these conferences also reflects the legitimization of hacking. While most hackers are becoming more involved in legitimate activities, hacking is an illegal act that can lead to arrest and prosecution. The fear of legal consequences prompted many of the respondents ($n = 79$) to incompletely take the online survey (mostly via snowballing). Also, some hackers tend to be more privacy sensitive and may have decided not to participate to protect their identity or intellectual property. There have been indications of hypocrisy in the hacker community, where Twitter, Facebook, and YouTube groups such as Anonymous and Lulzsec boast about their malicious accomplishments (Mansfield-Devine, 2011; Murphy, 2011). Many of these self-defined hackers also are fearful to take an anonymous online survey.

To partially mitigate these issues, recruitment was through a wide variety of sources and interviewed a diverse pool of participants to increase the likelihood that some relevant responses would be completed by at least one participant. The target population were offensive security engineers, who possess the same skill sets as hackers. Notably, many of the offensive researchers or hackers given the online survey face to face during Black Hat and DefCon (and sub-cons) were more comfortable in self-reporting their hacking experience.

It is well known that using self-reported data is biased, especially in studying anti-social and unethical behavior (Krumpal, 2013). Instead, scenario-based methods are more suitable to overcome such challenges by providing hypothetical situations (Pogarsky, 2004). In the field of IS, the scenario methods have been widely used to study various topics.

A fourth limitation is the use of the Dark Triad vs. the Dark Tetrad personality traits. Increasingly, scholars call for sadism as an addition to the Dark Triad in the study of antisocial and delinquent behaviors.

Finally, on sample size, age, and gender: The initial study intended to obtain 300 respondents; however, the final sample size was only 245 respondents, with only 89 fitting the combatants or hacker profile. These respondents also were intentionally solicited on websites where hacking was commonly discussed and promoted. The sample was not representative of all computer deviants or those that possess hacking skills, only the individuals who were on the chosen sites at the time of solicitation.

Despite these limitations, conducting research via the Internet provides researchers with the opportunity to investigate active users of computer deviancy within their own environment. Rather than a relaxing or forensic setting, the sample provides extensive information about those individuals that may use the Internet in a deviant manner for criminal behaviors while the person remains in his/her cyberspace atmosphere. Future psychological research conducted over the Internet in the area of cybercriminal behavior is possible and should continue, as there are an unlimited number of respondents in the realm of cyberspace all having the ability to provide psychological and behavioral information.

Future studies may wish to expand their sampling to include, not only non-computer deviants, but methods of gaining access to computer deviants who may not be members of the hacker community or subculture. Future studies also may want to include respondents under the age of 18 to identify computer deviants in the first stage of the Guttman-like progression (Hollinger, 1988). These respondents (“script kiddies”) may be found in capture the flag (CTF) or CyberPatriot communities or competitions.

Future research might also attempt to include data from other sources including peers and official reports. Although the target sample was selected for offensive security engineers, it is unlikely to contain many high-rate or serious offenders. Future research might be usefully conducted in samples with greater density of offending. These limitations, notwithstanding the

present results, provide additional validation for the CCI-R+, suggesting cyberstalking is relevant to computer criminal behavior.

There is an unchallenged increase in the prevalence of cybercrime, and as technology becomes more global, it will only be easier for individuals to engage in cyber-criminal behaviors. Future research should continue to assess the personality characteristics of computer deviants while distinguishing between the various types of computer-related crimes. As technology evolves, so does the cyber-criminal, and the types of cybercrimes will expand.

5.4 Summary

This study contributes to the emerging IS literature concerning the occurrence of cyber-criminal behavior from the perspective of individual personality factors, and the findings hold substantive implications, both theoretical and practical. The current study was unable to present evidence that people with high Dark Triad tendencies are more likely to engage in cyber-criminal behaviors. This may be due to response bias and the ability to answer honestly. It is with optimism that this study can provide some new insights and offer a valuable foundation for the future research on cybercriminals.

At present, the literature lacks empirical research on the hacker mindset, especially studies involving behavioral evidence on abilities and predispositions (Xu et al., 2013). Studies on hacking have typically focused on motivational aspects and general personality traits of the individuals who engage in hacking; little systematic research has been conducted on dispositional attributions that may be associated with the choice to pursue criminal indulgence.

Hackers continue to pose a serious threat to organizations. Security researchers can benefit from a greater understanding of how and why hackers engage in criminal behavior. A limiting

factor of such studies is the inability to verify that self-proclaimed hackers participating in research actually possess their purported knowledge and skills.

It may appear unusual to include psychological traits in a discussion about cyber-criminal behaviors, but like any other crime, people are involved, the inclusion of these behavioral science topics becomes self-evident. Computer crime is as much about the individuals involved in deviant behavior as it is about the technology (Furnell, 2003). Therefore, research focusing on people is vital if there is any real hope of facing the phenomena of cybercrime. This study adds to the growing body of knowledge in the area of identifying discriminant characteristics that can be used to help construct taxonomies and profiles for cybercriminals.

The implications of this study are promising, as behavioral information systems researchers operating in the information security space will directly benefit from expanding on this research. Furthermore, adaptations of this research have the potential to be utilized in a variety of contexts and in information systems research.

Appendix A
Data Collection
Online Survey Instrument



Dear Participant,

I am a PhD student in Information Systems/Information Security at the College of Engineering and Computing, Nova Southeastern University, working under the supervision of Dr. James L. Parrish. You are being asked to take this survey because your job functions incorporate specialized hacking skills, or you have an extensive hacking background, making you suitable for my survey. The purpose of this research study is to investigate different perspectives of personalities and behaviors within social networking sites (SNSs); focusing on the attribution of computer deviancy within SNSs.

The feedback that you provide will be used for this research study and used in aggregated form. Your participation in responding to this one-time survey should require less than 10 minutes of your time. This survey is completely voluntary with anonymity. You can decide not to participate in this research and exit the survey at any time. No personal identifiable information will be collected, and all your responses will be completely anonymous. Information we learn about you in this research study will be handled in a confidential manner, within the limits of the law. This data will be available to the researcher, the Institutional Review Board and other representatives of this institution. All confidential data will be kept securely on an encrypted storage device. All data will be kept for 36 months from the end of the study and destroyed after that time by disk sanitizing.

If you have questions, you can contact Kim Withers (kw954@mynsu.nova.edu / 210-373-0899) after business hours, or Dr. James Parrish at jlparish@nova.edu. If you have questions about the study but want to talk to someone else who is not a part of the study, you can call the Nova Southeastern University Institutional Review Board (IRB) at (954) 262-5369 or toll free at 1-866-499-0790 or email at IRB@nova.edu.

All responses in this survey are voluntary, but for the completeness of the data collection, please try to respond to all questions in the survey. Please feel free to forward this survey to any other friends or colleagues in your organization that may be suitable to answer the survey. Thank you in advance for your time and assistance. Thank you for taking the time to participate in my research study.

Regards,

Kim L. Withers

Computer Crime Index-Revised Plus (CCI-R+)

- ❖ CCI-R+ survey questions were removed from final dissertation report - permission for the instrument usage is required from author (see Appendix B).

Dark Triad Dirty Dozen (DTDD) Survey Instrument

Rate the following questions using a 5-point Likert scale 1 (Strongly agree) to 5 (Strongly disagree).

	Strongly Agree				Strongly Disagree
I tend to be unconcerned with the morality of my actions.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I have used deceit or lied to get my way.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I tend to want others to admire me.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I tend to exploit others towards my own end.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I tend to want others to pay attention to me.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I tend to lack remorse.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I tend to seek prestige or status.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I tend to be callous or insensitive.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I have used flattery to get my way.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I tend to manipulate others to get my way.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I tend to expect special favors from others.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I tend to be cynical.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Cyberstalking Survey Instrument

Rate the following questions using a 5-point frequency scale 1 (never) to 5 (6 or more times). Please answer whether you have ever done the following:

Post authentic materials but remark on them with false information to embarrass someone?

Never

Once

2 to 3 times

4 to 5 times

6 or more times

Deface/alter someone's online profile to create inaccurate or embarrassing information about the victim?

Never

Once

2 to 3 times

4 to 5 times

6 or more times

Secretly gather information about someone that could be used to harass them later?

Never

Once

2 to 3 times

4 to 5 times

6 or more times

Stolen or cloned someone's computer or another electronic device?

Never

Once

2 to 3 times

4 to 5 times

6 or more times

Modify a picture of someone to make them look worse on social media?

Never

Once

2 to 3 times

4 to 5 times

6 or more times

Make negative comments about someone on their social media account?

Never

Once

2 to 3 times

4 to 5 times

6 or more times

Use positioning software/mobile apps (i.e. GPS, Find Friends) to obtain someone's location information without their knowledge or permission?

Never

Once

2 to 3 times

4 to 5 times

6 or more times

Write threatening or menacing messages to someone online?

Never

Once

2 to 3 times

4 to 5 times

6 or more times

Post explicit photos of a person online without his/her consent?

Never

Once

2 to 3 times

4 to 5 times

6 or more times

Become fake “friends” with someone you do not like?

Never

Once

2 to 3 times

4 to 5 times

6 or more times

Send another person spyware to gather their personal data?

Never

Once

2 to 3 times

4 to 5 times

6 or more times

Pretend to be someone else (i.e. Catfish) to have a relationship online (e.g., different age, different gender)?

Never

Once

2 to 3 times

4 to 5 times

6 or more times

Repost inflammatory information or known rumors to embarrass someone?

Never

Once

2 to 3 times

4 to 5 times

6 or more times

Write highly negative responses to someone else's posts online or trolling?

Never

Once

2 to 3 times

4 to 5 times

6 or more times

Tweet or send misinformation/unethical content using a fake identity as an act of revenge?

Never

Once

2 to 3 times

4 to 5 times

6 or more times

Purposely send another person a computer virus to cause damage to their data or system?

Never

Once

2 to 3 times

4 to 5 times

6 or more times

Act as a fake friend to learn about someone?

Never

Once

2 to 3 times

4 to 5 times

6 or more times

Post truthful but negative or highly personal information about someone that he/she wants kept private?

Never

Once

2 to 3 times

4 to 5 times

6 or more times

Please supply the following Demographics.

What is your gender?

Male

Female

What is your age range?

18 - 24

25 - 34

35 - 44

45 - 54

55 - 64

65 or older

Thank you for taking the time to complete this survey! Your response has been recorded.

We would appreciate if you would recommend friends or colleagues to take this survey. You would be contributing to the data collection of this dissertation study tremendously.



Appendix B

Computer Crime Index -Revised Plus (CCI-R/CCI-R+)

Survey Instrument Permission

Request for CCI-R or CCI-RI Survey Instrument

[Report message](#) · [Block user](#)



Kim Withers

15 minutes ago

Mr. Rogers, my name is Kim Withers and I am a PhD student at Nova Southeastern University. I am interested in using your CCI-R or CCI-RI survey instrument in my current research. How do I send you a formal letter to have access to these instruments? I tried looking to see if they were free instruments, but could not find it anywhere. Can you help me? Thanks in advance.

Kim Withers



Marcus Rogers to you

Just now

Kim,

I will send you the instruments tomorrow morning. They are on a system in my lab.

[Reply](#)

[Mark as unread](#)

[Archive conversation](#)



Thank you so much Dr. Rogers for your prompt reply! I will look forward to it!

Kim Withers

CCI-R/CCI-RI Survey Instrument

Report message · Block user



Kim Withers

15 days ago

Hello, Dr. Seigfried-Spellar, my name is Kim Withers, and a PhD Student at Nova Southeastern University. I have cited some of your work in my current dissertation proposal. I had reached out to Dr. Marcus Rogers a few weeks ago about the use of the CCI-R instrument for my dissertation research, and he mentioned he had to send me from his lab. I have not heard back from him, assuming he has been busy traveling possibly. I noticed that you were a co-author on some works with him. I was wondering if you are also a co-author of the instrument? I was wondering if he was the only one that could provide the instrument. I am sorry to bother you, but I am under time constraints to provide a final draft dissertation proposal to my committee for review. Please advise and thanks in advance.

Kim



Kathryn C. Seigfried-Spellar to you

5 days ago

Here is the updated CCI-R+. You can cite it as: Seigfried-Spellar, K., Bays, J., Graziano, W., & Rogers, M.K. (In progress). Relating Person-Thing Orientation to Different Types of Computer Criminal Behaviors.

📎 CCI-R+ (2017) - Final.docx



Kim Withers

5 days ago

Oh my!!! Thank you so much! You have made me so happy today! I will revise my Dissertation Proposal tonight!

Appendix C

Company-Paid Approval to Conduct Data Collection



Thu 3/1/2018 10:28 AM

HARTEN, JOE

FW: Blackhat 2018 attendee list REXROAD

To: WETHERS, KIM; MUNISWAMY, MANJULA

You forwarded this message on 3/1/2018 10:44 AM.
This message was sent with High Importance.

Kim/Manjula-

FYI, you made the cut! Look out for something from Mark Kolaks. He coordinates the attendees.

Congrats...

-Joe

From: SZELES, ANN MARIE

Sent: Thursday, March 01, 2018 11:21 AM

To: CONNOR, COLIN R <col111@att.com>; HARTEN, JOE <jh1214@att.com>; BARRY, MICHELLE K <m3573@att.com>; NANASHKO, MICHAEL E <mnd1945@att.com>

Cc: SZELES, ANN MARIE <as1453@att.com>

Subject: Blackhat 2018 attendee list REXROAD

Importance: High

AE,

The below folks have been selected to attend the Blackhat/Defcon Event. Attendees should bring back something to share with others on tSpace – something they learned and think others would benefit. Mark Kolaks will be sending pertinent information shortly.

Please let your folks know they have been selected.

Thanks,

2018 Blackhat/DefCon Candidates

Name	Manager	Previously Attended/Comments
Austerweide, Jeff	Connor	No
Wethers, Kim	Harten	No data collection for dissertation
Muniswamy, Manjula	Harten	No
Ramachandran, Jay	Barry	No
Hochberg, Glenn	Nanashko	No

Thank you,

Ann Marie Szales

Appendix D

Participation Letter

Participant Letter for Anonymous Surveys NSU Consent to be in a Research Study Entitled

A Psychosocial Behavioral Attribution Model: Examining the Relationship Between the "Dark Triad" and Computer Deviant Behaviors Impacting Social Networking Sites

I am a Ph.D. student in Information Systems/Information Security at the College of Engineering and Computing, Nova Southeastern University, working under the supervision of Dr. James L. Parrish. You are being asked to take this survey because your job functions incorporate specialized hacking skills, or you have an extensive hacking background, making you suitable for my survey. The purpose of this research study to investigate different perspectives of personalities and behaviors within social networking sites (SNSs); focusing on the attribution of computer deviancy within SNSs.

The feedback that you provide will be used for this research study and used in aggregated form. Your participation in responding to this one-time survey should require less than 10 minutes of your time. This survey is completely voluntary with anonymity. You can decide not to participate in this research and exit the survey at any time. No personal identifiable information will be collected, and all your responses will be completely anonymous. Information we learn about you in this research study will be handled in a confidential manner, within the limits of the law. This data will be available to the researcher, the Institutional Review Board and other representatives of this institution. All confidential data will be kept securely on an encrypted storage device. All data will be kept for 36 months from the end of the study and destroyed after that time by disk sanitizing.

If you have questions, you can contact Kim Withers (kw954@mynsu.nova.edu / 210-373-0899) after business hours, or Dr. James Parrish at jlparrish@nova.edu. If you have questions about the study but want to talk to someone else who is not a part of the study, you can call the Nova Southeastern University Institutional Review Board (IRB) at (954) 262-5369 or toll free at 1-866-499-0790 or email at IRB@nova.edu.

All responses in this survey are voluntary, but for the completeness of the data collection, please try to respond to all questions in the survey. Please feel free to forward this survey to any other friends or colleagues in your organization that may be suitable to answer the survey. Thank you in advance for your time and assistance. Thank you for taking the time to participate in my research study.

Regards,

Kim L. Withers

Appendix E

Survey Recruitment Cards



VOLUNTEERS NEEDED FOR DOCTORAL RESEARCH STUDY

Personalities and Computer Deviant Behaviors in Social Media

We are conducting a doctoral dissertation research study to investigate different perspectives of personality traits and computer deviance within social networking sites (SNSs) and the impact on social media communities. This survey is conducted in affiliation with Nova Southeastern University, including Kim Withers acting as Primary Investigator, and James L. Parrish, Ph.D., acting as a Co-Investigator. Filling out the survey will take about 5 to 7 minutes. Participation is completely voluntary and anonymous. I am looking for individuals ages 18 and older, preferably with hacking experience. Thank you in advance for taking the time to participate in this research study. Please use the following link or scan the QR code with your mobile device to take the survey.

https://qplus.az1.qualtrics.com/jfe/form/SV_bpFZ6qHkYPTLOiL



Appendix F

IRB Approval Letter



MEMORANDUM

To: **Kim L. Withers, PhD Student DISS**

From: **Ling Wang, Ph.D.,
Center Representative, Institutional Review Board**

Date: **June 13, 2018**

Re: **IRB #: 2018-311; Title, "A Psychosocial Behavioral Attribution Model: Examining the Relationship Between the "Dark Triad" and Computer Deviant Behaviors Impacting Social Networking Sites"**

I have reviewed the above-referenced research protocol at the center level. Based on the information provided, I have determined that this study is exempt from further IRB review under **45 CFR 46.101(b) (Exempt 2: Interviews, surveys, focus groups, observations of public behavior, and other similar methodologies)**. You may proceed with your study as described to the IRB. As principal investigator, you must adhere to the following requirements:

- 1) **CONSENT:** If recruitment procedures include consent forms, they must be obtained in such a manner that they are clearly understood by the subjects and the process affords subjects the opportunity to ask questions, obtain detailed answers from those directly involved in the research, and have sufficient time to consider their participation after they have been provided this information. The subjects must be given a copy of the signed consent document, and a copy must be placed in a secure file separate from de-identified participant information. Record of informed consent must be retained for a minimum of three years from the conclusion of the study.
- 2) **ADVERSE EVENTS/UNANTICIPATED PROBLEMS:** The principal investigator is required to notify the IRB chair and me (954-262-5369 and Ling Wang, Ph.D., respectively) of any adverse reactions or unanticipated events that may develop as a result of this study. Reactions or events may include, but are not limited to, injury, depression as a result of participation in the study, life-threatening situation, death, or loss of confidentiality/anonymity of subject. Approval may be withdrawn if the problem is serious.
- 3) **AMENDMENTS:** Any changes in the study (e.g., procedures, number or types of subjects, consent forms, investigators, etc.) must be approved by the IRB prior to implementation. Please be advised that changes in a study may require further review depending on the nature of the change. Please contact me with any questions regarding amendments or changes to your study.

The NSU IRB is in compliance with the requirements for the protection of human subjects prescribed in Part 46 of Title 45 of the Code of Federal Regulations (45 CFR 46) revised June 18, 1991.

Cc: James Parrish, Ph.D.
Ling Wang, Ph.D.

References

- Abell, L., & Brewer, G. (2014). Machiavellianism, self-monitoring, self-promotion and relational aggression on Facebook. *Computers in Human Behavior*, 36, 258-262.
- Ackerman, M. S. (2004). Privacy in pervasive environments: next generation labeling protocols. *Personal and Ubiquitous Computing*, 8(6), 430-439.
- Acquisti, A., & Gross, R. (2006). Imagined communities: Awareness, information sharing, and privacy on the Facebook. In *International workshop on privacy enhancing technologies* (pp. 36-58). Springer Berlin Heidelberg.
- Ahn, H., Kwolek, E. A., & Bowman, N. D. (2015). Two faces of narcissism on SNS: The distinct effects of vulnerable and grandiose narcissism on SNS privacy control. *Computers in Human Behavior*, 45, 375-381.
- Aiken, L. S., & West, S. G. (1991). *Multiple regression: Testing and interpreting interactions*. Thousand Oaks, CA: Sage.
- Alexy, E. M., Burgess, A. W., Baker, T., & Smoyak, S. A. (2005). Perceptions of cyberstalking among college students. *Brief treatment and Crisis Intervention*, 5(3), 279.
- Allik, J., Laidra, K., Realo, A., & Pullmann, H. (2004). Personality development from 12 to 18 years of age: Changes in mean levels and structure of traits. *European Journal of Personality*, 18(6), 445-462.
- al-Khateeb, H., Alhaboby, Z. A., Barnes, J., Brown, A., Brown, R., Cobley, P., ... & Shukla, M. (2015). *A practical guide to coping with cyberstalking*. Andrews UK Limited, 2015.
- Allen, N. J., & Meyer, J. P. (1990). The measurement and antecedents of affective, continuance and normative commitment to the organization. *Journal of Occupational and Organizational Psychology*, 63(1), 1-18.
- Allport, G.W. & Odbert, H.S. (1936). Trait-names: A psycho-lexical study. *Psychological Monographs*, 47(211).
- American Psychiatric Association (2013). *Diagnostic and Statistical Manual of Mental Disorders*, (5th Ed.) Arlington, VA: American Psychiatric Association.
- Anderson, C. A., Krull, D. S., & Weiner, B. (1996). Explanations: Processes and consequences. In E. T. Higgins, & A. W. Kruglanski (Eds.), *Social psychology: Handbook of basic principles* (pp. 271-296). New York: Guilford Press.
- Anderson, J. C., & Gerbing, D. W. (1988). Structural equation modeling in practice: A review and recommended two-step approach. *Psychological Bulletin*, 103(3), 411.

- Ashton, M. C., Lee, K., Goldberg, L. R., & de Vries, R. E. (2009). Higher order factors of personality: Do they exist?. *Personality and Social Psychology Review*, 13(2), 79-91.
- Avolio, B. J., Yammarino, F. J., & Bass, B. M. (1991). Identifying common methods variance with data collected from a single source: An unresolved sticky issue. *Journal of Management*, 17(3), 571-587.
- Awang, Z. (2012). A handbook on SEM: Structural equation modelling. *Shah Alam, Selangor Darul Ehsan: UiTM*.
- Bachmann, M. (2010). The risk propensity and rationality of computer hackers. *International Journal of Cyber Criminology*, 4(1/2), 643.
- Bachrach, Y., Kosinski, M., Graepel, T., Kohli, P., & Stillwell, D. (2012). Personality and patterns of Facebook usage. In *Proceedings of the 4th Annual ACM Web Science Conference* (pp. 24-32). ACM.
- Backstrom, L., Boldi, P., Rosa, M., Ugander, J., & Vigna, S. (2012). Four degrees of separation. In *Proceedings of the 4th Annual ACM Web Science Conference* (pp. 33-42). ACM.
- Bandara, W., Miskon, S., & Fieft, E. (2011). A systematic, tool-supported method for conducting literature reviews in information systems. In *Proceedings of the 19th European Conference on Information Systems (ECIS 2011)*.
- Barker, V. (2009). Older adolescents' motivations for social network site use: The influence of gender, group identity, and collective self-esteem. *CyberPsychology and Behavior*, 12(2), 209-213.
- Barlett, C. P., & Gentile, D. A. (2012). Attacking others online: The formation of cyberbullying in late adolescence. *Psychology of Popular Media Culture*, 1(2), 123.
- Barnes, J., (2013). *Technological Profiling of Cyber-Bullying*. [Online] Available at: <https://www.forensicmag.com/article/2013/09/technological-profiling-cyber-bullying>
- Baron, M. A. (2008). Guidelines for writing research proposals and dissertations. *Division of Educational Administration: University of South Dakota*, 1-52.
- Bazarova, N. N., & Hancock, J. T. (2010). From Dispositional Attributions to Behavior Motives: The Folk-Conceptual Theory and Implications for Communication. *Annals of the International Communication Association*, 34(1), 63-91.
- Baughman, H. M., Jonason, P. K., Lyons, M., & Vernon, P. A. (2014). Liar pants on fire: Cheater strategies linked to the Dark Triad. *Personality and Individual Differences*, 71, 35-38.
- Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly*, 35(4), 1017-1042.

- Bergman, S. M., Fearing, M. E., Davenport, S. W., & Bergman, J. Z. (2011). Millennials, narcissism, and social networking: What narcissists do on social networking sites and why. *Personality and Individual Differences*, 50, 706–711.
- Black, P. J., Woodworth, M., & Porter, S. (2014). The Big Bad Wolf? The relation between the Dark Triad and the interpersonal assessment of vulnerability. *Personality and Individual Differences*, 67, 52-56.
- Board, B. J., & Fritzon, K. (2005). Disordered personalities at work. *Psychology, Crime and Law*, 11, 17–32.
- Bocij, P., & McFarlane, L. (2003). Cyberstalking: The technology of hate. *The Police Journal*, 76(3), 204-221.
- Bocij, P., & McFarlane, L. (2002). Online harassment: Towards a definition of cyberstalking. *Prison Service Journal*, 139, 31-38.
- Bocij, P., Griffiths, M. D., & McFarlane, L. (2002). Cyberstalking: A new challenge for criminal law. *The Criminal Lawyer*, 122, 3-5.
- Boddy, C. R., Ladyshewsky, R. K., & Galvin, P. (2010). The influence of corporate psychopaths on corporate social responsibility and organizational commitment to employees. *Journal of Business Ethics*, 97(1), 1-19.
- Bommer, M., Gratto, C., Gravander, J., & Tuttle, M. (1987). A behavioral model of ethical and unethical decision making. *Journal of Business Ethics*, 6(4), 265-280.
- Boochever, R. (2012). *Psychopaths online: Modeling psychopathy in social media discourse* (Honors thesis). Retrieved from <https://ecommons.cornell.edu/handle/1813/29536>
- Bossler, A. M., & Holt, T. J. (2009). On-line activities, guardianship, and malware infection: An examination of routine activities theory. *International Journal of Cyber Criminology*, 3(1), 400.
- Boudreau, M. C., Gefen, D., & Straub, D. W. (2001). Validation in information systems research: a state-of-the-art assessment. *MIS Quarterly*, 1-16.
- Boyd, D. M., & Ellison, N. B. (2007). Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication*, 13(1), 210-230.
- Bradley, G. W. (1978). Self-serving biases in the attribution process: A reexamination of the fact or fiction question. *Journal of Personality and Social Psychology*, 36(1), 56.
- Brown, S. (2006). The criminology of hybrids: Rethinking crime and law in technosocial networks. *Theoretical Criminology*, 10(2), 223-244.

- Brown, S. (2013). Virtual criminology. *The Sage dictionary of criminology*. In McLaughlin, E., & Muncie, J. (Eds.). (2012). *The Sage Dictionary of Criminology*. Sage.
- Browne, M. W., & Cudeck, R. (1993). Alternative ways of assessing model fit. *Sage Focus Editions*, 154, 136-136.
- Buffardi, L. E., & Campbell, W. K. (2008). Narcissism and social networking Web sites. *Personality and Social Psychology Bulletin*, 34, 1303-1314.
- Buonanno, P. (2003). The socioeconomic determinants of crime: A review of the literature. *University of Milan-Bicocca, Working Paper Series*, 63.
- Burger, J. M. (1993). *Personality* (3rd ed.). Pacific Grove, CA: Brooks/Cole.
- Byrne, B. M. (2013). *Structural equation modeling with LISREL, PRELIS, and SIMPLIS: Basic concepts, applications, and programming*. Psychology Press.
- Burton-Jones, A. (2009). Minimizing method bias through programmatic research. *MIS Quarterly*, 445-471.
- Buss, A. R. (1978). Causes and reasons in attribution theory: A conceptual critique. *Journal of Personality and Social Psychology*, 36, 1311-1321.
- Cao, J., Basoglu, K. A., Sheng, H., & Lowry, P. B. (2015). A Systematic Review of Social Networking Research in Information Systems.
- Campbell, D. T. (1960). Recommendations for APA test standards regarding construct, trait, or discriminant validity. *American Psychologist*, 15(8), 546-553.
- Campbell, Q., & Kennedy, D. M. (2009). The psychology of computer criminals. *Computer Security Handbook*, 40-160.
- Campbell, W. K., Foster, C. A., & Finkel, E. J. (2002). Does self-love lead to love for others? A story of narcissistic game playing. *Journal of Personality and Social Psychology*, 83, 340-354.
- Carver, C. S., & Scheier, M. F. (2000). *Perspectives on personality* (4th ed.). Boston: Allyn and Bacon.
- Chabrol, H., Van Leeuwen, N., Rodgers, R., & Séjourné, N. (2009). Contributions of psychopathic, narcissistic, Machiavellian, and sadistic personality traits to juvenile delinquency. *Personality and Individual Differences*, 47(7), 734-739.
- Charoensukmongkol, P. (2016). Exploring personal characteristics associated with selfie-taking. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, 10(2).
- Chaubey, R. K. (2009). *An Introduction to Cyber Crime and Cyber Law*. Kamal Law House.

- Chiesa, Raoul, Stefania Ducci, and Silvio Ciappi. 2009. *Profiling hackers: The science of criminal profiling as applied to the world of hacking*. Boca Raton, FL: Auerbach Publications.
- Chin, W. W., Marcolin, B. L., & Newsted, P. R. (2003). A partial least squares latent variable modeling approach for measuring interaction effects: Results from a Monte Carlo simulation study and an electronic-mail emotion/adoption study. *Information Systems Research*, 14(2), 189-217.
- Chin, W. W. (1998). The partial least squares approach to structural equation modeling. *Modern Methods for Business Research*, 295(2), 295-336.
- Christie, R., & Geis, F. (1970). *Studies in Machiavellianism*. New York, NY: Academic Press.
- Cook, T. D., & Campbell, D. T. (1979). *Quasi-experimentation: Design and analysis issues for field settings*. Boston: Houghton Mifflin.
- Clark, L. A., & Watson, D. (1995). Constructing validity: Basic issues in objective scale development. *Psychological Assessment*, 7(3), 309.
- Clarke, R.V. (2004). Technology, criminology, and crime science. *European Journal on Criminal Policy and Research*, 10(1), 55–63.
- Cleckley, H. M. (2016). *The mask of sanity: An attempt to clarify some issues about the so-called psychopathic personality 3rd edition*. Pickle Partners Publishing.
- Coleman, G. (2010). The hacker conference: A ritual condensation and celebration of a lifeworld. *Anthropological Quarterly*, 47-72.
- Creswell, J. W., & Creswell, J. D. (2017). *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage Publications.
- Cronbach, L. J. (1951). Coefficient alpha and the internal structure of tests. *Psychometrika*, 16(3), 297-334.
- Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security*, 32, 90-101.
- Day C., Kowalenko S., Ellis M., Dawe S., Harnett P., Scott S. (2011). The helping families programme: A new parenting intervention for children with severe and persistent conduct problems. *Child and Adolescent Mental Health*, 16, 167-171.
- DeLisi, M. (2016). Why Psychopathy as Unified Theory of Crime?. In *Psychopathy as Unified Theory of Crime* (pp. 1-13). Palgrave Macmillan US.

- Dempsey, A. G., Sulkowski, M. L., Dempsey, J., & Storch, E. A. (2011). Has cyber technology produced a new group of peer aggressors? *CyberPsychology, Behavior, and Social Networking*, 14(5), 297-302.
- Davis, K. E., Ace, A., & Andra, M. (2000). Stalking perpetrators and psychological maltreatment of partners: Anger-jealousy, attachment insecurity, need for control, and break-up context. *Violence and Victims*, 15(4), 407-425.
- DeHue, F., Bolman, C., & Völlink, T. (2008). Cyberbullying: Youngsters' experiences and parental perception. *CyberPsychology & Behavior*, 11(2), 217-223.
- Dijkstra, T. K. (2010). Latent variables and indices: Herman Wold's basic design and partial least squares. In *Handbook of partial least squares* (pp. 23-46). Springer, Berlin, Heidelberg.
- Douceur, J. R. (2002). The sybil attack. In *International Workshop on Peer-to-Peer Systems* (pp. 251-260). Springer, Berlin, Heidelberg.
- Edunov, S., Diuk, C., Filiz, I. O., Bhagat, S., & Burke, M. (2016). Three and a half degrees of separation. *Research at Facebook*.
- Elsa, K. K. (1995). The juvenile crime debate: Rehabilitation, punishment, or prevention. *Kan. JL & Pub. Pol'y*, 5, 135.
- Emmons, R. A. (1984). Factor analysis and construct validity of the Narcissistic Personality Inventory. *Journal of Personality Assessment*, 48, 291-300.
- Fanti, K. A., Demetriou, A. G., & Hawa, V. V. (2012). A longitudinal study of cyberbullying: Examining risk and protective factors. *European Journal of Developmental Psychology*, 9(2), 168-181.
- Field, A. (2009). *Discovering statistics using SPSS*. Sage publications.
- Federal Bureau of Investigation. (2016). 2015 Internet Crime Report. Retrieved from https://www.ic3.gov/media/annualreport/2015_IC3Report.pdf
- Ferrell, O. C., & Gresham, L. G. (1985). A contingency framework for understanding ethical decision making in marketing. *The Journal of Marketing*, 87-96.
- Fire, M., Goldschmidt, R., & Elovici, Y. (2014). Online social networks: threats and solutions. *IEEE Communications Surveys & Tutorials*, 16(4), 2019-2036.
- Fischbacher-Smith, D. (2015). The enemy has passed through the gate: Insider threats, the dark triad, and the challenges around security. *Journal of Organizational Effectiveness: People and Performance*, 2(2), 134-156.
- Fiske, S. T., & Taylor, S. E. (2013). *Social cognition: From brains to culture*. Sage.

- Foulkes, L., McCrory, E. J., Neumann, C. S., & Viding, E. (2014). Inverted social reward: Associations between psychopathic traits and self-report and experimental measures of social reward. *PloS One*, 9(8), e106000.
- Fox, K. A., Nobles, M. R., & Fisher, B. S. (2011). Method behind the madness: An examination of stalking measurements. *Aggression and Violent Behavior*, 16(1), 74-84.
- Fox, J., & Rooney, M. C. (2015). The Dark Triad and trait self-objectification as predictors of men's use and self-presentation behaviors on social networking sites. *Personality and Individual Differences*, 76, 161-165.
- Franke, G., & Sarstedt, M. (2018). Heuristics Versus Statistics in Discriminant Validity Testing: A Comparison of Four Procedures. *Internet Research*, forthcoming.
- Freud, S. (1923). A neurosis of demoniacal possession in the seventeenth century. *Collected Papers*, 4, 436-472.
- Furnell, S. (2003). Cybercrime: vandalizing the information society. *Web Engineering*, 333-365.
- Garcia, D., & Sikström, S. (2014). The dark side of Facebook: Semantic representations of status updates predict the Dark Triad of personality. *Personality and Individual Differences*, 67, 92-96.
- Gefen, D., Rigdon, E. E., & Straub, D. (2011). Editor's comments: an update and extension to SEM guidelines for administrative and social science research. *MIS Quarterly*, iii-xiv.
- Gefen, D., & Straub, D. (2005). A practical guide to factorial validity using PLS-Graph: Tutorial and annotated example. *Communications of the Association for Information Systems*, 16(1), 5.
- Gefen, D., Straub, D., & Boudreau, M. C. (2000). Structural equation modeling and regression: Guidelines for research practice. *Communications of the Association for Information Systems*, 4(1), 7.
- Gjelten, T. (2013). First strike: US cyber warriors seize the offensive. *World Affairs*, 33-43.
- Goga, O., Venkatadri, G., & Gummadi, K. P. (2015). The doppelgänger bot attack: Exploring identity impersonation in online social networks. In *Proceedings of the 2015 ACM Conference on Internet Measurement Conference* (pp. 141-153). ACM, New York, NY, USA, 141-153.
- Gold, A. H., Malhotra, A., & Segars, A. H. (2001). Knowledge management: An organizational capabilities perspective. *Journal of Management Information Systems*, 18(1), 185-214.
- Gonzalez, J. J., & Sawicka, A. (2002). A framework for human factors in information security. In *WSEAS International Conference on Information Security, Rio de Janeiro* (pp. 448-187).

- Görzig, A., & Ólafsson, K. (2013). What makes a bully a cyberbully? Unravelling the characteristics of cyberbullies across twenty-five European countries. *Journal of Children and Media*, 7(1), 9-27.
- Goodboy, A. K., & Martin, M. M. (2015). The personality profile of a cyberbully: Examining the Dark Triad. *Computers in Human Behavior*, 49, 1-4.
- Gothard, S., Viglione Jr, D. J., Meloy, J. R., & Sherman, M. (1995). Detection of malingering in competency to stand trial evaluations. *Law and Human Behavior*, 19(5), 493.
- Gove, W. R. (1985). *The effect of age and gender on deviant behavior: A biopsychosocial perspective*. In A. Rossi (Ed.), *Gender and the life course* (pp. 115-144). Chicago: Aldine.
- Grabosky, P. N., & Smith, R. G. (1998). *Crime in the digital age: Controlling telecommunications and cyberspace illegalities*. Transaction Publishers.
- Graham, J. M. (2006). Congeneric and (essentially) tau-equivalent estimates of score reliability: What they are and how to use them. *Educational and Psychological Measurement*, 66(6), 930-944.
- Green, S. B., & Yang, Y. (2009). Commentary on coefficient alpha: A cautionary tale. *Psychometrika*, 74(1), 121-135.
- Greitzer, F. L., & Frincke, D. A. (2010). Combining traditional cyber security audit data with psychosocial data: towards predictive modeling for insider threat mitigation. In *Insider Threats in Cyber Security* (pp. 85-113). Springer US.
- Greitzer, F. L., & Hohimer, R. E. (2011). Modeling human behavior to anticipate insider attacks. *Journal of Strategic Security*, 4(2), 25.
- Grimmelmann, J. (2010). The Internet is a semicommons. *Fordham Law Review*, 78, 2799.
- Hair, J. F., Hult, G. T., Ringle, C. M., & Sarstedt, M. (2017). *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)* (2e ed.). Thousand Oaks: Sage.
- Hair Jr, J. F., Hult, G. T. M., Ringle, C., & Sarstedt, M. (2016). *A primer on partial least squares structural equation modeling (PLS-SEM)*. Sage Publications.
- Hair J. F., Sarstedt, M., Hopkins, L., & G. Kuppelwieser, V. (2014). Partial least squares structural equation modeling (PLS-SEM) An emerging tool in business research. *European Business Review*, 26(2), 106-121.
- Hair, J. F., Black, W. C., Babin, B. J., Anderson, R. E., & Tatham, R. L. (1998). *Multivariate data analysis* (Vol. 5, No. 3, pp. 207-219). Upper Saddle River, NJ: Prentice hall.

- Hajlo, N., Nejad, M. A. G., Jangi, S., & Hossain, S. A. (2015). Relationship between the dark triad personality and cyber bullying in student internet users. *Journal of Kermanshah University of Medical Sciences*, 19(1), 24-31.
- Hare, R. D. (1996). Psychopathy a clinical construct whose time has come. *Criminal Justice and Behavior*, 23(1), 25-54. [41]
- Hare, R. D. (2003). *The Hare Psychopathy Checklist-Revised*. (PCL-R; 2nd Ed.). Toronto, Canada: Multi-Health Systems.
- Hare, R. D., Clark, D., Grann, M., & Thornton, D. (2000). Psychopathy and the predictive validity of the PCL-R: An international perspective. *Behavioral Sciences & the Law*, 18(5), 623-645.
- Hamburger, Y. A., & Ben-Artzi, E. (2000). The relationship between extraversion and neuroticism and the different uses of the Internet. *Computers in Human Behavior*, 16(4), 441-449.
- Hamilton, D. L. (1998). Dispositional and attributional inferences in person perception. In J. M. Darley & J. Cooper (Eds.), *Attribution and social interaction: The legacy of Edward E. Jones* (pp. 99-114). Washington, DC: American Psychological Association.
- Harrison, A., Summers, J., & Mennecke, B. (2016). The effects of the dark triad on unethical behavior. *Journal of Business Ethics*, 1-25.
- Heider, F. (1958). *The psychology of interpersonal relations*. New York: Wiley.
- Henseler, J., Hubona, G., & Ray, P. A. (2016). Using PLS path modeling in new technology research: updated guidelines. *Industrial Management & Data Systems*, 116(1), 2-20.
- Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science*, 43(1), 115-135.
- Henseler, J., Dijkstra, T. K., Sarstedt, M., Ringle, C. M., Diamantopoulos, A., Straub, D. W., Ketchen, D. J., Hair, J. F., Hult, G. T. M., & Calantone, R. J. (2014). Common beliefs and reality about partial least squares: comments on Rönkkö & Evermann (2013). *Organizational Research Methods*, 17(2), 182-209.
- Henseler, J., & Sarstedt, M. (2013). Goodness-of-fit indices for partial least squares path modeling. *Computational Statistics*, 28(2), 565-580.
- Henseler, J., Ringle, C. M., & Sinkovics, R. R. (2009). The use of partial least squares path modeling in international marketing. *Advances in International Marketing*, 20, 277-320.
- Hinduja, S., & Patchin, J. W. (2008). Cyberbullying: An exploratory analysis of factors related to offending and victimization. *Deviant Behavior*, 29(2), 129-156.

- Hoffman, C. (2013). Hacker Hat Colors Explained: Black Hats, White Hats, and Gray Hats. *How-To Geek*, April, 20.
- Hofstee, W. K. B. (1994). Who should own the definition of personality? *European Journal of Personality*, 8, 149–162.
- Hollinger, R. C. (1988). Computer hackers follow a Guttman-like progression. *Sociology and Social Research*, 72(3), 199-200.
- Holt, T. J. (2007). Subcultural evolution? Examining the influence of on-and off-line experiences on deviant subcultures. *Deviant Behavior*, 28(2), 171-198.
- Holt, T. J. (2012). Exploring the intersections of technology, crime, and terror. *Terrorism and Political Violence*, 24, 337-354.
- Holt, T. J., Blevins, K. R., & Burkert, N. (2010). Considering the pedophile subculture online. *Sexual Abuse*, 22, 3-24.
- Holt, T. J., & Bossler, A. M. (2009). Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. *Deviant Behavior*, 30, 1-25.
- Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2015). *Cybercrime and Digital Forensics: An introduction*. Routledge.
- Holtfreter, K., Reisig, M. D., & Pratt, T. C. (2008). Low self-control, routine activities, and fraud victimization. *Criminology*, 46, 189-220.
- Hu, T., Poston, R.S. and Kettinger, W.J. (2011). Nonadopters of online social network services: Is it easy to have fun yet? *Communications of the Association for Information Systems*, 29 (1), 441-458.
- Hu, L. T., & Bentler, P. M. (1999). Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Structural Equation Modeling: A Multidisciplinary Journal*, 6(1), 1-55.
- Hunker, J., & Probst, C. W. (2011). Insiders and insider threats-an overview of definitions and mitigation techniques. *JoWUA*, 2(1), 4-27.
- Jakobwitz, S., & Egan, V. (2006). The dark triad and normal personality traits. *Personality and Individual Differences*, 40(2), 331-339.
- Jessor, R., & Jessor, S. L. (1977). Problem behavior and psychosocial development: A longitudinal study of youth.
- Johnson, M., Egelman, S., & Bellovin, S. M. (2012). Facebook and privacy: it's complicated. In *Proceedings of the Eighth Symposium on Usable Privacy and Security* (p. 9). ACM.

- Joinson, A. N. (2005). Deviance and the internet: New challenges for social science. *Social Science Computer Review*, 23(1), 5–7.
- Jolliffe, D., & Farrington, D. P. (2011). Is low empathy related to bullying after controlling for individual and social background variables? *Journal of Adolescence*, 34(1), 59-71.
- Jonason, P. K., Kaufman, S. B., Webster, G. D., & Geher, G. (2013). What Lies Beneath the Dark Triad Dirty Dozen: Varied Relations with the Big Five. *Individual Differences Research*, 11(2).
- Jonason, P. K., Li, N. P., & Buss, D. M. (2010). The costs and benefits of the Dark Triad: Implications for mate poaching and mate retention tactics. *Personality and Individual Differences*, 48(4), 373-378.
- Jonason, P. K., Li, N. P., Webster, G. D., & Schmitt, D. P. (2009). The dark triad: Facilitating a short-term mating strategy in men. *European Journal of Personality*, 23(1), 5-18.
- Jonason, P. K., & Luévano, V. X. (2013). Walking the thin line between efficiency and accuracy: Validity and structural properties of the Dirty Dozen. *Personality and Individual Differences*, 55(1), 76-81.
- Jonason, P. K., & McCain, J. (2012). Using the HEXACO model to test the validity of the Dirty Dozen measure of the Dark Triad. *Personality and Individual Differences*, 53(7), 935-938.
- Jonason, P. K., & Webster, G. D. (2010). The dirty dozen: A concise measure of the dark triad. *Psychological Assessment*, 22(2), 420.
- Jones, C. M. (2005). Genetic and Environmental Influences on Criminal Behavior. *British Medical Journal*.
- Jones, D. N., & Figueredo, A. J. (2013). The core of darkness: Uncovering the heart of the Dark Triad. *European Journal of Personality*, 27(6), 521-531.
- Jones, E. E., & Nisbett, R. E. (1971). *The actor and the observer: Divergent perceptions of the causes of behavior*. New York, NY, United States: General Learning Press.
- Jones, E. E., Kanouse, D., Kelley, H. H., Nisbett, R. E., Valins, S., & Weiner, B. (Eds.). (1972). *Attribution: Perceiving the causes of behavior*. Morristown, NJ: General Learning Press.
- Jordan, T., & Taylor, P. (1998). A sociology of hackers. *The Sociological Review*, 46(4), 757-780.
- Judge, T. A., & Bono, J. E. (2000). Five-factor model of personality and transformational leadership. *Journal of Applied Psychology*, 85(5), 751.
- Junglas, I. A., Johnson, N. A., & Spitzmüller, C. (2008). Personality traits and concern for privacy: an empirical study in the context of location-based services. *European Journal of Information Systems*, 17(4), 387-402.

- Kajonius, P. J., Persson, B. N., & Jonason, P. K. (2015). Hedonism, achievement, and power: universal values that characterize the Dark Triad. *Personality and Individual Differences*, 77, 173-178.
- Kajonius, P. J., Persson, B. N., Rosenberg, P., & Garcia, D. (2016). The (mis) measurement of the Dark Triad Dirty Dozen: exploitation at the core of the scale. *PeerJ*, 4, e1748.
- Kelley, H. H. (1967). Attribution theory in social psychology. In D. Levine (Ed.), *Nebraska Symposium on Motivation* (Vol. 15, pp. 129-238). Lincoln: University of Nebraska Press.
- Kierkegaard, S. (2008). Cybering, online grooming and age play. *Computer Law & Security Review*, 24(1), 41-55.
- Kirwan, G., & Power, A. (2012). Can Theories of Crime be Applied to Cybercriminal Acts?. In *The Psychology of Cyber Crime: Concepts and Principles* (pp. 37-51). IGI Global.
- Kline, R. B. (2015). *Principles and practice of structural equation modeling*. Guilford Publications.
- Kosinski, M., Bachrach, Y., Kohli, P., Stillwell, D., & Graepel, T. (2014). Manifestations of user personality in website choice and behavior on online social networks. *Machine Learning*, 95(3), 357-380.
- Kropp, P. R., Hart, S. D., Lyon, D. R., & Storey, J. E. (2011). The development and validation of the guidelines for stalking assessment and management. *Behavioral Sciences & the Law*, 29(2), 302-316.
- Krueger, R. F., Eaton, N. R., Clark, L. A., Watson, D., Markon, K. E., Derringer, J., ... & Livesley, W. J. (2011a). Deriving an empirical structure of personality pathology for DSM-5. *Journal of Personality Disorders*, 25(2), 170-191.
- Krueger, R., Eaton, N., Derringer, J., Markon, K., Watson, D., & Skodol, A. (2011b). Personality in the DSM-5: Helping delineate personality disorder content and framing the metastructure. *Journal of Personality Assessment*, 93, 325-331.
- Krumpal, I. (2013). Determinants of social desirability bias in sensitive surveys: a literature review. *Quality & Quantity*, 47(4), 2025-2047.
- Kumari, P. (2010). Requirements analysis for privacy in social networks. In *8th International Workshop for Technical, Economic and Legal Aspects of Business Models for Virtual Goods*, Namur.
- Labuschagne, W. B. L. (2004). A COMPARATIVE FRAMEWORK FOR EVALUATING INFORMATION SECURITY RISK MANAGEMENT METHODS. *Standard Bank Academy for Information Technology*, Rand Afrikaans University.

- Langton, Lynn and Katrina Baum. (2010). *Identity Theft Reported by Households*, 2007. Washington, DC: US Department of Justice.
- Larsen, R. J., & Buss, D. M. (2010). *Personality psychology: Domains of knowledge about human nature* (4th International Student Ed.). New York, NY: McGraw-Hill.
- Lauritsen, J. L., Laub, J. H., & Sampson, R. J. (1992). Conventional and delinquent activities: Implications for the prevention of violent victimization among adolescents. *Violence and Victims*, 7(2), 91-108.
- Leedy, P.D. & Ormrod, J. E. (2010) *Practical Research: Planning and Design*, Ninth Edition. NYC: Merrill.
- Levy, S. (1984). *Hackers: Heroes of the computer revolution* (Vol. 14). Garden City, NY: Anchor Press/Doubleday.
- Lindsay, M., & Krysik, J. (2012). Online harassment among college students: A replication incorporating new Internet trends. *Information, Communication & Society*, 15(5), 703-719.
- Loper, D. K. (2001). The criminology of computer hackers: A qualitative and quantitative analysis.
- Lowry, P., Zhang, J., Wang, C., Wu, T., & Siponen, M. (2013). Understanding and Predicting Cyberstalking in Social Media: Integrating Theoretical Perspectives on Shame, Neutralization, Self-Control, Rational Choice, and Social Learning.
- Luppici, Rocci. (2009). Technoethical inquiry: From technological systems to society. *Global Media Journal – Canadian Edition*, 2(1), 5-21.
- Lyytinen, K., & King, J. L. (2004). Nothing at the center? Academic legitimacy in the information systems field. *Journal of the Association for Information Systems*, 5(6), 8.
- Maasberg, M., Warren, J., & Beebe, N. L. (2015). The dark side of the insider: Detecting the insider threat through examination of Dark Triad personality traits. In *System Sciences (HICSS), 2015 48th Hawaii International Conference* (pp. 3518-3526). IEEE.
- Madge, Clare. (2007). Developing a geographers' agenda for online research ethics. *Progress in Human Geography*, 31(5), 654-674.
- Magklaras, G. B., & Furnell, S. M. (2001). Insider threat prediction tool: Evaluating the probability of IT misuse. *Computers & Security*, 21(1), 62-73.
- Mahmut, M. K., Menictas, C., Stevenson, R. J., & Homewood, J. (2011). Validating the factor structure of the Self-Report Psychopathy Scale in a community sample. *Psychological Assessment*, 23, 670.

- Mairesse, F., & Walker, M. (2006). Words mark the nerds: Computational models of personality recognition through language. In *Proceedings of the 28th Annual Conference of the Cognitive Science Society* (pp. 543-548).
- Menesini, E., & Spiel, C. (2012). Introduction: Cyberbullying: Development, consequences, risk and protective factors. *European Journal of Developmental Psychology*, 9(2), 163-167.
- Malle, B. F. (2004). *How the mind explains behavior: Folk explanations, meaning, and social interaction*. Cambridge, MA: MIT Press.
- Marshall, M. N. (1996). Sampling for qualitative research. *Family Practice*, 13(6), 522-526.
- Marshall, P. D., & Barbour, K. (2015). Making intellectual room for persona studies: a new consciousness and a shifted perspective.
- Maslow, A. H. (1943). A theory of human motivation. *Psychological Review*, 50(4), 370.
- McCrae, R. R., & John, O. P. (1992). An introduction to the five-factor model and its applications. *Journal of Personality*, 60(2), 175-215.
- McDonald, R. P. (1996). Path analysis with composite variables. *Multivariate Behavioral Research*, 31(2), 239-270.
- McDonald, S., Hope, N. H., Strom, K. J., & Pope, M. W. (2009). The impact of the Internet on deviant behavior and deviant communities. *Durham, NC: The Institute for Homeland Security Solution*.
- McHoskey, J. W., Worzel, W., & Szyarto, C. (1998). Machiavellianism and psychopathy. *Journal of Personality and Social Psychology*, 74, 192-210.
- McHoskey, J. (1995). Narcissism and machiavellianism. *Psychological Reports*, 77(3), 755-759.
- McKirnan, D. (1980). The identification of deviance: A conceptualization and initial test of a model of social norms. *European Journal of Social Psychology*, 10(1), 75-93.
- Melander, L. A. (2010). College students' perceptions of intimate partner cyber harassment. *Cyberpsychology, Behavior, and Social Networking*, 13(3), 263-268.
- Ménard, K. S., & Pincus, A. L. (2012). Predicting overt and cyber stalking perpetration by male and female college students. *Journal of Interpersonal Violence*, 27(11), 2183-2207.
- Meloy, J. R. (2001). *The psychology of stalking: Clinical and forensic perspectives*. Academic Press.
- Miller, D. T., & Ross, M. (1975). Self-serving biases in the attribution of causality: Fact or fiction. *Psychological Bulletin*, 82(2), 213-225.

- Millon, T., & Grossman, S. (2007). *Moderating severe personality disorders: A personalized psychotherapy approach*. John Wiley & Sons.
- Minei, Elizabeth & Matusitz, Jonathan. (2011). Cyberterrorist messages and their effects on targets: A qualitative analysis. *Journal of Human Behavior in the Social Environment*, 21, 995-1019.
- Mislove, A., Post, A., Druschel, P., & Gummadi, P. K. (2008). Ostra: leveraging trust to thwart unwanted communication. In *NSDI* (Vol. 8, pp. 15-30).
- Molavi Kakhki, A., Kliman-Silver, C., & Mislove, A. (2013). Iolaus: Securing online content rating systems. In *Proceedings of the 22nd International Conference on World Wide Web* (WWW '13). ACM, New York, NY, USA, 919-930.
- Mondal, M., Viswanath, B., Clement, A., Druschel, P., Gummadi, K. P., Mislove, A., & Post, A. (2012). Defending against large-scale crawls in online social networks. In *Proceedings of the 8th International Conference on Emerging Networking Experiments and Technologies* (CoNEXT '12). ACM, New York, NY, USA, 325-336.
- Moore, M. (2011). Psychological theories of crime and delinquency. *Journal of Human Behavior in the Social Environment*, 21(3), 226-239.
- Morley, K., & Hall, W. (2003). Is there a genetic susceptibility to engage in criminal acts? *Australian Institute of Criminology: Trends and Issues in Crime and Criminal Justice*, 263, 1-6.
- Muris, P., Merckelbach, H., Otgaar, H., & Meijer, E. (2017). The malevolent side of human nature: A meta-analysis and critical review of the literature on the dark triad (narcissism, Machiavellianism, and psychopathy). *Perspectives on Psychological Science*, 12(2), 183-204.
- Narayanan, A., & Shmatikov, V. (2008). Robust de-anonymization of large sparse datasets. In *2008 IEEE Symposium on Security and Privacy (sp 2008)* (pp. 111-125). IEEE.
- Narayanan, A., & Shmatikov, V. (2009). De-anonymizing social networks. In *2009 30th IEEE Symposium on Security and Privacy* (pp. 173-187). IEEE.
- Nathanson, C., Paulhus, D. L., & Williams, K. M. (2006). Predictors of a behavioral measure of scholastic cheating: Personality and competence but not demographics. *Contemporary Educational Psychology*, 31(1), 97-122.
- Nevin, A. D. (2015). *Cyber-psychopathy: Examining the relationship between dark e-personality and online misconduct* (Doctoral dissertation). University of Western Ontario, [Location].
- Nurse, J. R., Buckley, O., Legg, P. A., Goldsmith, M., Creese, S., Wright, G. R., & Whitty, M. (2014a). Understanding insider threat: A framework for characterizing attacks. In *Security and Privacy Workshops (SPW), 2014 IEEE* (pp. 214-228). IEEE.

- Nurse, J. R., Legg, P. A., Buckley, O., Agraftiotis, I., Wright, G., Whitty, M., & Creese, S. (2014b). A critical reflection on the threat from human insiders—its nature, industry perceptions, and detection approaches. In *International Conference on Human Aspects of Information Security, Privacy, and Trust* (pp. 270-281). Springer International Publishing.
- O'Boyle Jr, E. H., Forsyth, D. R., Banks, G. C., & McDaniel, M. A. (2012). A meta-analysis of the dark triad and work behavior: A social exchange perspective. *Journal of Applied Psychology*, 97(3), 557.
- Ogilvie, E. (2000). Cyberstalking. *Trends and Issues in Crime and Criminal Justice/Australian Institute of Criminology*, (166), 1.
- Parrish Jr, J. L., Bailey, J. L., & Courtney, J. F. (2009). A Personality Based Model for Determining Susceptibility to Phishing Attacks. *Little Rock: University of Arkansas*
- Paulhus, D. L. (2001). Normal narcissism: Two minimalist accounts. *Psychological Inquiry*, 12(4), 228-230.
- Paulhus, D. L., & Jones, D. N. (2011). Introducing a short measure of the Dark Triad. In *Poster presentation at the meeting of the Society for Personality and Social Psychology*, San Antonio, CA, USA.
- Paulhus, D. L., & Williams, K.M. (2002). The Dark Triad of personality. *Journal of Research in Personality*, 36, 556-563.
- Perren, S., Corcoran, L., Cowie, H., Dehue, F., Garcia, D., Mc Guckin, C., et al. (2012). Tackling cyberbullying: Review of empirical evidence regarding successful responses by students, parents, and schools. *International Journal of Conflict and Violence*, 6(2), 283–293.
- Pew Internet Research (2016). Facebook usage and engagement is on the rise, while adoption of other platforms holds steady. Retrieved from: <http://www.pewinternet.org/2016/11/11/social-media-update-2016/>
- Pittaro, M. L. (2007). Cyber stalking: An analysis of online harassment and intimidation. *International Journal of Cyber Criminology*, 1(2), 180-197.
- Podsakoff, P. M., MacKenzie, S. B., & Podsakoff, N. P. (2012). Sources of method bias in social science research and recommendations on how to control it. *Annual Review of Psychology*, 63, 539-569.
- Podsakoff, P. M., MacKenzie, S. B., Lee, J. Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology*, 88(5), 879.
- Podsakoff, P. M., & Organ, D. W. (1986). Self-reports in organizational research: Problems and prospects. *Journal of management*, 12(4), 531-544.

- Polaschek, D. L., & Daly, T. E. (2013). Treatment and psychopathy in forensic settings. *Aggression and Violent Behavior, 18*(5), 592-603.
- Raskin, R., & Terry, H. (1988). A principal-components analysis of the Narcissistic Personality Inventory and further evidence of its construct validity. *Journal of Personality and Social Psychology, 54*, 890-902.
- Rauthmann, J. F., & Kolar, G. P. (2012). How “dark” are the Dark Triad traits? Examining the perceived darkness of narcissism, Machiavellianism, and psychopathy. *Personality and Individual Differences, 53*(7), 884-889.
- Reid, J. (1995). Demographic and Clinical Comparison of Obsessional. *American Journal of Psychiatry, 152*, 258-263.
- Rhee, S. H., & Waldman, I. D. (2002). Genetic and environmental influences on antisocial behavior: A meta-analysis of twin and adoption studies. *Psychological Bulletin, 128*, 490-529.
- Rid, Thomas. (2012). Cyber war will not take place. *The Journal of Strategic Studies, 35*, 5-32.
- Riek, M., Böhme, R., & Moore, T. (2014). Understanding the influence of cybercrime risk on the e-service adoption of European Internet users. In *13th Workshop on the Economics of Information Security*.
- Ringle, C. M., Wende, S., & Becker, J. M. (2015). SmartPLS 3. Boenningstedt: SmartPLS GmbH, <http://www.smartpls.com>.
- Ringle, C.M., Sarstedt, M., & Straub, D.W. (2012). A critical look at the use of PLS-SEM in MIS Quarterly. *MIS Quarterly, 36*(1), iii-xiv.
- Rogers, M. K. (2001). A social learning theory and moral disengagement analysis of criminal computer behavior: An exploratory study.
- Rogers, M. K. (2006). A two-dimensional circumplex approach to the development of a hacker taxonomy. *Digital investigation, 3*(2), 97-102.
- Rogers, M. K., Seigfried, K., & Tidke, K. (2006a). Self-reported computer criminal behavior: A psychological analysis. *Digital Investigation, 3*, 116-120.
- Rogers, M., Smoak, N., & Liu, J. (2006b). Self-reported deviant computer behavior. *Deviant Behavior, 27*(3), 245-268.
- Ross, C., Orr, E. S., Sisic, M., Arseneault, J. M., Simmering, M. G., & Orr, R. R. (2009). Personality and motivations associated with Facebook use. *Computers in Human Behavior, 25*(2), 578-586.

- Ross, S. R., Lutz, C. J., & Bailey, S. E. (2004). Psychopathy and the five factor model in a noninstitutionalized sample: a domain and facet level analysis. *Journal of Psychopathology and Behavioral Assessment*, 26, 213–223.
- Rotter, J. B. (1954). *Social learning and clinical psychology*. Prentice-Hall. Englewood Cliffs, NJ.
- Schell, B. H., & Dodge, J. L. (2002). *The hacking of America: Who's doing it, why, and how*. Greenwood Publishing Group Inc.
- Schultz, E. E. (2002). A framework for understanding and predicting insider attacks. *Computers & Security*, 21(6), 526-531.
- Seebruck, R. (2015) A typology of hackers: Classifying cyber malfeasance using a weighted arc circumplex model. *Digital Investigation*, 14, 36-45.
- Seigfried-Spellar, K., Bays, J., Graziano, W., & Rogers, M.K. (In progress). Relating Person-Thing Orientation to Different Types of Computer Criminal Behaviors.
- Seigfried-Spellar, K. C., O'Quinn, C. L., & Treadway, K. N. (2015). Assessing the relationship between autistic traits and cyberdeviancy in a sample of college students. *Behaviour & Information Technology*, 34(5), 533-542.
- Seigfried-Spellar, K. C., & Treadway, K. N. (2014). Differentiating hackers, identity thieves, cyberbullies, and virus writers by college major and individual differences. *Deviant Behavior*, 35(10), 782-803.
- Seigfried-Spellar, K. C., Villacís-Vukadinović, N., & Lynam, D. R. (2017). Computer criminal behavior is related to psychopathy and other antisocial behavior. *Journal of Criminal Justice*, 51, 67-73.
- Sekaran, U., & Bougie, R. (2016). *Research methods for business: A skill building approach*. John Wiley & Sons.
- Sheridan, L. P., & Grant, T. (2007). Is cyberstalking different?. *Psychology, crime & law*, 13(6), 627-640.
- Sireci, S. G. (1998). The construct of content validity. *Social indicators research*, 45(1-3), 83-117.
- Sledgianowski, D., & Kulviwat, S. (2009). Using social network sites: The effects of playfulness, critical mass and trust in a hedonic context. *Journal of Computer Information Systems*, 49(4), 74-83.
- Smith, R. (2010). Identity theft and fraud. *The handbook of internet crime*. Devon: Willan Publishing, pp. 273-301.
- Smith, S. F., & Lilienfeld, S. O. (2013). Psychopathy in the workplace: The knowns and unknowns. *Aggression and Violent Behavior*, 18(2), 204-218.

- Spain, S. M., Harms, P., & LeBreton, J. M. (2014). The dark side of personality at work. *Journal of Organizational Behavior*, 35(S1), S41-S60.
- Spertus, E., (1991), 'Why are there so few female computer scientists?', unpublished paper, MIT.
- Spitzberg, B. H., & Manusov, V. (2014). Attribution Theory. *Engaging Theories in Interpersonal Communication: Multiple Perspectives*, 37.
- Storey, J. E., Hart, S. D., Meloy, J. R., & Reavis, J. A. (2009). Psychopathy and stalking. *Law and Human Behavior*, 33(3), 237-246.
- Sukhai, N. B. (2004). Hacking and cybercrime. In *Proceedings of the 1st Annual Conference on Information Security Curriculum Development* (pp. 128-132). ACM.
- Sumner, C., Byers, A., Boochever R., & Park, G.J. (2012). Predicting dark triad personality traits from twitter usage and a linguistic analysis of tweets. *11th International Conference on Machine Learning and Applications*, Boca Raton, FL, pp. 386-393.
- Tajfel, H., & Turner, J. C. (1986). The social identity theory of inter group behavior in S Worchel & WG Austin (Eds) *Psychology of intergroup relations*. Chicago: Nelson.
- Taylor, R.W., Fritsch, E.J., & Liederbach, J. (2014). *Digital Crime and Digital Terrorism* (3rd ed.). Prentice Hall Press, Upper Saddle River, NJ, USA.
- Tetlock, P. E., & McGuire, C. (1986). Cognitive perspectives on foreign policy. *Psychology and the Prevention of Nuclear War*, 1, 255-273.
- Teo, T. S. H., Srivastava, S. C., & Jiang, L. (2008). Trust and electronic government success: an empirical study. *Journal of Management Information Systems*, 25(3), 99–132.
- Thambusamy, R. & Nemati, H., (2011). A sociomateriality practice perspective of online social Networking. *ICIS 2011 Proceedings*. 27.
- Tokunaga, R. S. (2010). Following you home from school: A critical review and synthesis of research on cyberbullying victimization. *Computers in Human Behavior*, 26(3), 277-287.
- Trevino, L. K. (1986). Ethical decision making in organizations: A person-situation interactionist model. *Academy of Management Review*, 11(3), 601-617.
- Turan, N., Polat, O., Karapirli, M., Uysal, C., & Turan, S. G. (2011). The new violence type of the era: Cyberbullying among university students: Violence among university students. *Neurology, Psychiatry and Brain Research*, 17(1), 21-26.
- Turkle, S. (1984). *The second self: Computers and the human spirit*. New York: Simon & Schuster.
- Turkle, S. (2005). *The second self: Computers and the human spirit*. MIT Press.

- Twenge, J. M., & Campbell, W. K. (2003). "Isn't it fun to get the respect that we're going to deserve?" Narcissism, social rejection, and aggression. *Personality and Social Psychology Bulletin*, 29, 261–272.
- Veselka, L., Schermer, J. A., & Vernon, P. A. (2012). The Dark Triad and an expanded framework of personality. *Personality and Individual Differences*, 53(4), 417–425.
- Viswanath, B., Bashir, M. A., Crovella, M., Guha, S., Gummadi, K. P., Krishnamurthy, B., & Mislove, A. (2014). Towards Detecting Anomalous User Behavior in Online Social Networks. In *USENIX Security Symposium* (pp. 223–238).
- Vogt, W. P., & Johnson, R. B. (2011). *Dictionary of statistics & methodology: a nontechnical guide for the social sciences: a nontechnical guide for the social sciences*. Sage.
- Wald, R., Khoshgoftaar, T. M., Napolitano, A., & Sumner, C. (2012). Using Twitter content to predict psychopathy. In *Machine Learning and Applications (ICMLA), 2012 11th International Conference on* (Vol. 2, pp. 394–401). IEEE.
- Weiner, B. (1980). The role of affect in rational (attributional) approaches to human motivation. *Educational Researcher*, 9(7), 4–11.
- Weiner, B. (1985). An attributional theory of achievement motivation and emotion. *Psychological Review*, 92(4), 548.
- Widiger, T. A. (1992). Categorical versus dimensional classification: Implications from and for research. *Journal of Personality Disorders*, 6, 287–300.
- Williams, K. M., Paulhus, D. L., & Hare, R. D. (2007). Capturing the four-factor structure of psychopathy in college students via self-report. *Journal of Personality Assessment*, 88, 205–219.
- Williams, K. M., McAndrew, A., Learn, T., Harms, P., & Paulhus, D. L. (2001). The Dark Triad returns: Entertainment preferences and antisocial behavior among narcissists, Machiavellians, and psychopaths. In *Poster presented at the 109th Annual Convention of the American Psychological Association, San Francisco, CA*.
- Williams, L. J., Cote, J. A., & Buckley, M. R. (1989). Lack of method variance in self-reported affect and perceptions at work: Reality or artifact? *Journal of Applied Psychology*, 74, 462–468.
- Williams, M. (2006). *Virtually criminal: Crime, deviance and regulation online*. Routledge.
- Woodworth, R. S. (1918). *Dynamic psychology*. New York: Columbia University Press.
- Xu, Z., Hu, Q., & Zhang, C. (2013). Why computer talents become computer hackers. *Communications of the ACM*, 56(4), 64–74.

- Zhang, S., Yu, L., Wakefield, R. L., & Leidner, D. E. (2016). Friend or Foe: Cyberbullying in Social Network Sites. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems*, 47(1), 51-71.
- Zheleva, E., & Getoor, L. (2009). To join or not to join: the illusion of privacy in social networks with mixed public and private user profiles. In *Proceedings of the 18th International Conference on World Wide Web* (pp. 531-540). ACM.
- Zhong, B., Hardin, M., & Sun, T. (2011). Less effortful thinking leads to more social networking? The associations between the use of social network sites and personality traits. *Computers in Human Behavior*, 27(3), 1265-1271.
- Zmud, R. W. (1979). Individual differences and MIS success: A review of the empirical literature. *Management Science*, 25(10), 966-979.
- Zuckerman, M. (1979). Attribution of success and failure revisited, or: The motivational bias is alive and well in attribution theory. *Journal of Personality*, 47(2), 245-287.