


8-2018

Juvenile Hackers: An Empirical Test of Self-Control Theory and Social Bonding Theory

Follow this and additional works at: <http://vc.bridgew.edu/ijcic>

 Part of the [Criminology Commons](#), [Criminology and Criminal Justice Commons](#), [Information Security Commons](#), and the [Psychology Commons](#)

Recommended Citation

Back, Sinchul; Soor, Sadhika; and LaPrade, Jennifer (2018) "Juvenile Hackers: An Empirical Test of Self-Control Theory and Social Bonding Theory," *International Journal of Cybersecurity Intelligence & Cybercrime*: 1(1), 40-55.

Available at: <http://vc.bridgew.edu/ijcic/vol1/iss1/5>

Copyright © 2018 Sinchul Back, Sadhika Soor, and Jennifer LaPrade

S. Back, S. Soor, & J. LaPrade (2018). *International Journal of Cybersecurity Intelligence and Cybercrime*, 1 (1), 40-55.

Juvenile Hackers: An Empirical Test of Self-Control Theory and Social Bonding Theory

Sinchul Back*, Florida International University, U.S.A

Sadhika Soor, Florida International University, U.S.A

Jennifer LaPrade, University of Texas at Dallas, U.S.A

Key Words: computer hacking, juvenile, self-control, social bonding

Abstract:

In accordance with a similar growth in information technology, computer hacking has become a pervasive issue as a form of crime worldwide in recent years. Self-control theory and social bonding theory have frequently been employed to explain various types of crimes, but rarely to explore computer hacking. Drawing from Gottfredson and Hirschi's (1990) self-control theory and Hirschi's (1969) social bonding theory, the purpose of this study is to empirically examine the suitability of these two theories in explaining juvenile computer hacking offenses. The self-report survey data utilized for the present study was derived from middle school and high school students in the United States, Venezuela, Spain, France, Germany, Poland, Hungary, and Russia. The current study hypothesizes that hackers' self-control and social bonding are significant predictors for the commission of computer hacking offenses. The findings of this study provide strong support for Gottfredson and Hirschi's (1990) self-control theory. In addition, the findings can be interpreted as partially supportive of Hirschi's (1969) social bonding theory. The authors conclude with a discussion on policy implications.

Introduction

Due to the advent of highly advanced information technologies (computer and network systems, internet, etc.), cybercriminals are able to easily leverage these cutting-edge technologies to commit computer hacking. Computer hacking is defined as a deviant act that is "analogous to the crime of trespass; it engages in a violation of a use restriction on the property that is committed by someone who has no right to access the property" (Brenner, 2010, pp. 50-51). According to former FBI Director James Comey and former Acting Assistant Attorney General for National Security Mary McCord (Department of Justice [DOJ], Office of Public Affairs, 2017), computer hacking and cybercrime are threats to the United States' national security and prosperity. For example, four Russian cybercriminals hacked Yahoo's systems to steal information from at least 500 million Yahoo accounts in 2014,

*Corresponding author

Sinchul Back, M.A., Department of Criminology and Criminal Justice, Steven J. Green School of International and Public Affairs, Florida International University, 11200 SW 8th St., PCA-257, Miami, FL 33199.

Email: sback008@fiu.edu

Reproduction, posting, transmission or other distribution or use of the article or any material therein, in any medium as permitted by written agreement of the International Journal of Cybersecurity Intelligence and Cybercrime, requires credit to the Journal as follows: "This Article originally appeared in International Journal of Cybersecurity Intelligence and Cybercrime (IJCIC), [year] Vol. #, Iss. #, pp. 00-00" and notify the Journal of such publication.

© 2018 IJCIC 2578-3289/2018/08

International Journal of Cybersecurity Intelligence and Cybercrime, Vol. 1, Iss. 1, Page. 40-55, Publication date: August 2018.

and a U.S. grand jury has indicted these hackers for computer hacking and economic espionage (DOJ, Office of Public Affairs, 2017). As another example of computer hacking, a hacker in Kentucky pleaded guilty to hacking a high school sports website and harassing and intimidating the website owner and others (DOJ, U.S. Attorney's Office, 2017). Former U.S. President Barack Obama stated that the global cost of hacking was estimated around 1 trillion (Menn, 2013). According to the Center for Strategic and International Studies' annual report (Simon, 2017), computer hacking incidents cause a 100 billion annual loss to the U.S. economy. In light of these incidents and damages, computer hacking has become a pervasive issue in the information era.

With that in mind, computer hacking has received considerable academic attention over the past decade, and issues of cybersecurity are highlighted by governments, international organizations, the private sector, and civil society (Bachmann, 2010; Hoffman, Rosenberg, Dodge, & Ragsdale, 2005). Scholars have strived to articulate the phenomenon of computer hacking and cybercriminal behaviors in the digital realm. A large body of research has focused on exploring hacker cultures, hackers' characteristics, hackers' perceptions, types of hackers, as well as hackers' techniques (e.g., Bachmann, 2010; Chua & Holt, 2016; Jordan & Taylor, 1998; Steinmetz & Gerber, 2015; Turgeman-Goldschmidt, 2005; Turgeman-Goldschmidt, 2008; Yar, 2005; Zhang, Young, & Prybutok, 2008). In the field of criminology, Gottfredson and Hirschi's (1990) general theory of crime and Hirschi's (1969) social bonding theory are two criminological theories that have been used to explain a number of different crime types. Nevertheless, to date, few studies have empirically examined Gottfredson and Hirschi's (1990) general theory of crime and Hirschi's (1969) social bonding theory to explain the phenomenon of computer hacking. Thus, the present study seeks to provide an empirical test of the effect of low self-control and social bonding on juvenile computer hacking.

The following sections present an overview of computer hacking and other related issues. A review of the relevant literature, including both self-control theory and social bonding theory, is presented in order to elaborate on the topic of this study. This study then explains the methodology and data collection that are used to test our hypotheses. Lastly, a theoretical analysis of the results is provided to offer suggestions for future research and possible policy implications.

Literature Review

As computer hacking has become more prevalent, researchers have also increasingly studied computer hackers to explain this phenomenon. Before adding to this literature with the current study, it is important to review what we generally know about computer hackers. To provide a better understanding of hackers, we broadly explore the research on hackers, and motivations of hackers.

Over the past decade, several scholars have attempted to conduct research about hackers and hacking phenomenon using qualitative or quantitative studies. In the study of *Craft(y)ness: An ethnographic study of hacking*, Steinmetz (2015) established a grounded understanding of "the hacker" using ethnographic field research and content analysis. Similarly, Steinmetz and Gerber (2015) examined how hackers perceive the hacker, hacking phenomenon, law enforcement, and privacy by employing a content analysis of the US-based magazine *2600: The Hacker Quarterly*. Chua and Holt (2016) conducted research on a cross-national examination of the techniques of neutralization to account for hacking behaviors among samples from colleges in the United States, Taiwan, and South Africa. They confirmed that there are "differences in the neutralizations and definitions associated with both hacking and malware use as well as regional influences on offending" (Chua & Holt, 2016, p. 534). Bachmann (2010) examined two personality characteristics commonly ascribed to hackers, and

they strived to reveal how these personality traits influence hacking activities. The findings of Bachmann's study determined that two personality characteristics (rationality and risk propensity) have significant importance for the prediction of hacking-related outcomes. Using nine different measures, including digital piracy measures, three fraud measures, one spam variable, and one malware variable, Kigerl (2016) investigated K-means clustering with a sample of 190 countries. Kigerl asserted that nations can be broken into low cybercrime countries, non-serious cybercrime countries, advance fee fraud countries, and phishing-scam countries.

Some scholars specifically portrayed young people's computer hacking (e.g., Bowker, 1999; DeMarco, 2001; Muncie, 1999; Verton, 2002; Yar, 2005). Initially, Yar (2005) explored a broad range of the existing literature regarding computer hacking to delineate juveniles' disproportionate involvement in cyber delinquency. Sterling (1994) argued that most hackers start to commit computer hacking between ages 11-18, and their aspiration for committing hacking decreases by their early twenties. In line with Sterling's assertion, Yar (2005) found that a period of inevitable psychological turmoil and crisis, as an adolescent, is a key factor that encourages juvenile hackers to engage in computer hacking. Hollin (2002) asserted that juvenile hackers tend to have a moral immaturity in which they are likely to behave upon their hedonistic impulses without considering rewards or losses from computer hacking. Similarly, DeMarco (2001) contended that an ethical deficit in a juvenile is strongly associated with the commission of computer-related crimes. Interestingly, Verton (2002) found that computer-addicted juvenile hackers are similar to juveniles who are addicted to marijuana, crack cocaine, and heroin.

Motivations of Hackers

An understanding of hackers' motivations is important for the theoretical framework at hand. Low self-control and a diminished bond to conventional society may increase an individual's propensity to engage in deviance. "Hacker culture" refers to a created underground community through which individuals with similar interests provide support, exchange skills, and network amongst one another (Turgeman-Goldschmidt, 2005). In this respect, hackers and their motivations should be understood within the context of a larger hacker culture, to which the hacker's bond may be stronger than conventional bonds. Further, cybercrime is deviant in nature and hacking specifically contains severe security threats. Bachmann (2010) found that hackers have a higher propensity to engage in risky behaviors than the general population. Further research has established links between cybercrime and other indications of antisocial behavior (e.g., Bowker, 1999; DeMarco, 2001; Muncie, 1999; Verton, 2002; Yar, 2005). Given the empirical associations between low self-control and cybercrime (Hinduja & Ingram, 2008; Holt, Bossler, & May, 2012), it is useful to examine hacking motivations with such relationships in mind. As such, in studying the motivations of computer hackers, Shoemaker and Kennedy (2009) have suggested that there are six major motivations; 1) revenge, 2) exposure, 3) hacktivism, 4) ego, 5) monetary gain, and 6) entertainment, which encourage cybercriminals to commit computer hacking.

First, some hackers who want revenge tend to show destructive behavior to release their anger towards other online users or organizations (Choi, 2015; Shoemaker & Kennedy, 2009). According to Turgeman-Goldschmidt (2005), hackers can retaliate against their target by using malicious code attacks (Holt & Schell, 2010). For example, if a former employee of the organization has been terminated from his/her contract by an organization, he/she can access the organization's network to set malicious code in order to destroy the organization's computer/network systems or commit a data breach for monetary gain (Choi, 2015).

Second, hackers or hacker groups commit cybercrimes and cyberattacks to show off their expertise in cyber space and gain exposure (Choi, 2015; Shoemaker & Kennedy, 2009). In fact, they attack famous organizations in private sectors or government computer/network systems in hopes of maximizing media coverage of the attack.

Third, hacktivism (political purpose) is a significant factor, which can drive hackers to commit a crime. Hacktivism combines the term of “hack” with the term of ‘activism’ (Choi, 2015). They are hackers with state-sponsorship or terrorism that demonstrate aggressive behavior to destroy their enemy’s infrastructure or critical computer/network systems that are directly connected with national security or their economic well-being. These types of hackers or hacker groups are generally motivated by ideologies of politics, religion or terrorism (Choi, 2015; Shoemaker & Kennedy, 2009).

Fourth, hackers can be motivated by ego, which may lead them to remain in a hacker subculture (Holt, 2016; Kigerl, 2016). Overcoming technical obstacles and creating advanced-level toolkits to solve the problems in hacker communities, hackers and hacker groups give them personal satisfaction because it makes them feel important and powerful (Holt, 2011). Also, hackers trespass and exploit the vulnerability of computer systems to boost their ego by using some types of hacking techniques (i.e., application layers, viruses, and DDoS attacks) (Choi, 2015).

Fifth, monetary gain can strongly drive hackers to commit a crime online. Usually, motivated hackers have the desire to gain profit through their skills to exploit individual online users, private sectors, and public sectors (Holt, 2011). Many hackers utilize phishing mailing, social engineering scams, password attacks, and ransomware scams in order to obtain valuable data and information they can use for financial gain. For example, a “Mafia Soldier” is a type of hacker driven by obtaining money, who generally works in organized crime groups (Choi, 2015; Shoemaker & Kennedy, 2009).

Sixth, entertainment is another significant motive that can make hackers actively engage in committing a crime in the cyber world. Hackers or hacking groups feel excited and have an adrenaline rush when attacking intended targets since “the final objective appears to be more playful than destructive” (Holt, 2011, p. 44; Kigerl, 2016). In other words, entertainment/excitement drives hackers to persistently implement exploitation and breach other users and the organizations’ assets online. In accordance with this view, juvenile hackers are more likely to commit computer hacking because juvenile hackers could have a higher propensity to engage in risky behaviors for their entertainment and excitement than the general population. Next, this study explores two theoretical frameworks – self-control theory and social bonding theory – and the applications of these two theories in the existing literature for both traditional crime and computer-related offenses.

Self-Control Theory

Gottfredson and Hirschi’s (1990) self-control theory, has become one of the dominant explanations of cybercrime (Agnew, 1991; Akers, 2013; Higgins, 2006; Holt, Bossler, & May, 2012). The theory assumes that all individuals are self-interested and inclined to commit a crime when the opportunity arises. It is self-control that inhibits the non-offender from engaging in delinquent behavior, while the offender’s low self-control causes the delinquent act to occur. Therefore, according to the theory, low self-control is the primary cause of all delinquent and criminal behavior across all cultures, places, and times. The theory assumes that rational individuals weigh the potential pleasure of an act against the potential pain of an act (Gottfredson & Hirschi, 1990; Meldrum, 2008; Schaefer, Vito, Marcum, Higgins, & Ricketts, 2015). In Gottfredson and Hirschi’s (1990) view, when the potential pleasure of an act outweighs the potential pain of an act, persons will choose pleasurable acts over painful acts

(Higgins, 2006). They contend that self-control impacts the probability of crime; those individuals with lower levels of self-control are more likely to engage in the commission of a crime. Gottfredson and Hirschi (1990) argue that individuals with low self-control are characterized as being impulsive, insensitive, short-sighted, nonverbal, and risk-takers who prefer simple tasks. Through a meta-analysis, Pratt and Cullen (2000) found that low self-control increases involvement in criminal behavior in the physical world. In online settings, individuals with low self-control are more likely to engage in computer hacking or cybercrime. In support of this argument, Holt, Bossler, and May (2012) found that low self-control was significantly associated with the commission of hacking and other forms of cyber deviance among a sample of juveniles. Marcum and associates (2014) also established a link between self-control and juvenile hacking. They found that low self-control is a significant predictor of online hacking behaviors, specifically Facebook account hacking and unauthorized website hacking (Marcum, Higgins, Ricketts, & Wolfe, 2014).

It is important to note that low self-control has been utilized to examine various types of cyber-crime, including digital piracy (e.g., Higgins, Wolfe, & Marcum, 2008; Hinduja & Ingram, 2008; Higgins, 2006; Higgins & Wilson, 2006; Moon, McCluskey, & McCluskey, 2010), and cyber-interpersonal violence, such as cyberbullying and cyberstalking (e.g., Vazsonyi, Machackova, Sevcikova, Smahel, & Cerna, 2012; Bossler & Holt, 2010). However, despite the increasing number of studies using self-control theory principles to explain digital piracy or cyber-interpersonal violence, empirical research on computer hacking is still relatively scarce (Bossler & Holt, 2010; Holt & Schell, 2010). Thus, the current study seeks to investigate whether or not low self-control influences the likelihood of computer hacking.

Social Bonding Theory

Social bonding theory, as put forth by Hirschi (1969), asserts that antisocial behavior is a result of an individual's weak ties to conventional society. Such ties are collectively referred to as the social bond, which is comprised of four elements, as outlined by Hirschi (1969). The first element, attachment, refers to the emotional ties an individual has with valued and significant others. The second element is a commitment, corresponding to an investment in conventional goals, such as academic or career aspirations. The third element of the social bond is that of involvement, which concerns the extent to which an individual participates in conventional activities. The final element, belief, refers to the acceptance of conventional norms and morals. Taken together, these four elements represent the social bond of Hirschi's (1969) control theory. The stronger an individual's bonds to society, the less likely he/she will be to deviate from societal norms. Social bonding theory contends that its four elements are interdependent, and the cumulative effect of the four said bonds is larger than their individual impacts (Hirschi, 1969). Further, if one of the four bonds deteriorates, the individual is at an increased likelihood of engaging in the antisocial behavior (Hirschi, 1969).

While self-control theory has been utilized to explain various types of crime, social bonding theory has rarely been used to investigate causal factors of cybercrime. In this regard, the existing literature has mainly focused on using social bonding to explain crimes in the physical world. For example, a number of empirical studies have supported the contention that weak social bonds contribute to an increased likelihood of engaging in delinquency (e.g., Agnew, 1991; Gentina & Singh, 2015; Huebner & Betts, 2002; Veenstra, Lindenberg, Tinga, & Ormel, 2010; Wiatrowski, Griswold, & Roberts, 1981; Yuksek & Solakoglu, 2016). Both Wiatrowski et al. (1981) and Agnew (1991) measured delinquency using self-report scales that asked participants about involvement in conventional crime, such as theft, assaults, and robbery. While Agnew (1991) ascertained that delinquent peer association, an element

outside of the social bond, had the greatest effect on delinquency, commitment to school nonetheless remained a significant predictive factor of delinquency. Correspondingly, Mesch (2009) found that the social bond elements of school attachment reduced the likelihood of regular cyber-pornography consumption among a sample of adolescents. Another study of adolescents by Chan and Wong (2015) found that weakened family attachment placed an individual at greater risk for bullying perpetration and bullying victimization. Furthermore, Hart and Mueller (2013) found that for both males and females, involvement in school-sponsored activities, as well as parental involvement, both had strong relationships to delinquency, suggesting the importance of time invested into pro-social activities. In line with this view of terrestrial crimes and social bonding, juvenile hackers' social bonding with their parents and schools must be an important predictor of criminal behavior (i.e., computer hacking) in the virtual world. For example, Bae (2017) found that social bonds, as well as self-control, decreased the likelihood of hacking and other online deviant behaviors among a sample of youth. While self-control was a strong predictor of cybercrime, Bae (2017) found that parental attachment and appropriate parental supervision had a significant effect on the likelihood of engaging in hacking and other cybercrimes.

In a longitudinal study examining the suitability of self-control theory and social bonding theory in explaining crime, Wright and colleagues (1999) found that individuals with low self-control had weakened bonds to school, less work successes, and diminished family ties (Wright, Caspi, Moffitt, & Silva, 1999). Wright's (1999) research contended that even when controlling for low self-control, social bonds remained a significant predictor of criminal behavior. Li (2004) found that among the social bonds, belief had the strongest impact on crime. Low self-control, however, had a more prominent effect on crime than the social bonds, but the cumulative effect of the social bonds produced a more robust impact on crime than self-control independently (Li, 2004). Overall, similar to the literature assessing low self-control and social bonds to explain crime in the physical and digital realm, the current study attempts to reveal whether or not low self-control and social bonding are associated with computer hacking among juveniles from eight countries.

Present Study

Some scholars argue that traditional criminological theories, occasionally, would not be suitable to explain cybercrime if terrestrial and virtual crimes were substantially different (Bossler & Burruss, 2012; Wall, 2007). Thus, if the current study can apply traditional criminological theories to explain crime in the digital realm, it will be beneficial to provide support for the literature. In light of this benefit, the purpose of this study is to empirically test whether both self-control and social bonding theories can be used to explain computer hacking. In addition, this study aims to explore the characteristics of each country's juvenile hackers, notably the effect of self-control and social bonding factors on computer hacking. Using responses from a nonrandom sample of 18,985 adolescents from eight countries, this study investigates these expectations. As a result, the current study contributes to theoretical examinations of cybercrime using self-control and social bonding theories. Furthermore, it will assist in revealing the characteristics of eight countries' (USA, Venezuela, Spain, France, Germany, Poland, Hungary, and Russia,) juvenile hackers. Unlike most physical crimes, computer hacking offenders can potentially cause damage anywhere in the world; therefore, it is important to study computer hackers on an international scale. To fill in gaps of the existing literature, the following hypotheses are evaluated in the present study:

Hypothesis 1: Higher levels of low self-control will increase computer hacking.

Hypothesis 2: Higher levels of parent attachment will decrease computer hacking.

Hypothesis 3: Higher levels of attachment to parental supervision will decrease computer hacking.

Hypothesis 4: Higher levels of involvement will decrease computer hacking.

Hypothesis 5: Higher levels of school attachment will decrease computer hacking.

Methods

Data

The cross-sectional data utilized in this study are derived from the second International Self-Report Delinquency Study (ISR2), a large international collaborative project investigating adolescent deviant behaviors, including computer hacking (ISR2, n.d.). The ISR2 indicates that the data collection was completed in 31 countries (grouped by geographical regions such as Asia, Europe, North America, and Latin America). In line with this data collection, China was the only Asian country in the dataset; however, none of the data related to Chinese juvenile hackers exists in the dataset. Participants in the self-report survey were 68,507 students from grades 7, 8 and 9 between the ages of 12 – 15 years old. The surveys were administered between 2005 and 2007 to random samples in the classrooms by researchers or teachers. An average of approximately 2,100 students were surveyed per country, most by using pencil and paper interview (PAPI), however computerized surveys were used in three countries (Finland, Switzerland, and Denmark). In each country, data collectors used a stratified random selection technique to ensure classrooms from metropolitan areas, mid-size cities, and small towns were equally represented in the final sample.

For this study, researchers opted to examine responses from students in eight countries—the United States, Venezuela, Spain, France, Germany, Poland, Hungary, and Russia. This is because these eight countries recently have been ranked and represented as the top 20 nations by count: perpetrators of cybercrime, as declared by several sources: 1) the Annual Internet Crime Reports published in partnership with the Internet Crime Complaint Center (IC3) and the Federal Bureau of Investigation (FBI), and 2) global cyber-threat reports by multinational cybersecurity companies such as Kaspersky Lab, and Norse (Cyberthreat real-time map, 2018; Internet Crime Complaint, 2009, 2010, 2011; Real-time visibility into global cyberattacks, 2018). The breakdown of the number of students surveyed by countries is as follows: 2,400 students were surveyed from the United States, 2,322 from Venezuela, 1,789 from Spain, 3,022 from France, 3,478 from Germany, 1,458 from Poland, 2,203 from Hungary, and 2,313 from Russia. This resulted in a total of 18,985 students for the sample size of this study. The United States data came from students in four states—Illinois, Massachusetts, New Hampshire, and Texas.

Measures

Dependent variable. The commission of computer hacking is the dependent variable for this study. The computer hacking measure is based on the computer hacking measure used by Holt, Bossler, and May (2012), and Marcum et al. (2014), and Udris (2016). The respondents were asked, “Did you do hacking during the last 12 months?” The item scale for the dependent variable was dichotomously coded (0 = no experience, 1 = experience) to measure hacking offenses among adolescents.

Independent variables. There are five independent variables used in this study. The five independent variables were: 1) low self-control, 2) attachment to parents, 3) attachment to parent supervision, 4) involvement, and 5) school attachment. Each independent variable in this study was

created through factor analysis. The first is a measure of low self-control (Cronbach’s Alpha = .785). A risk-taking subscale was utilized to measure self-control levels (Grasmick, Tittle, Bursik, & Arneklev, 1993). The respondents were presented with the statements: “I like to test myself every now and then by doing something a little risky,” “Sometimes I will take a risk just for the fun of it,” and “Excitement and adventure are more important to me than security.”

Next, the nine items of the social bonding scale were comprised of four subscales: 1) attachment to parents (two items: “How do you usually get along with your father?” and “How do you usually get along with your mother?”), 2) attachment to parental supervision (two items: “Do your parents usually know who you are with when you go out?” and “When you go out at night do your parents generally tell you at what time you have to be back?”), 3) involvement (two items: “How often do you and your parents do something together, such as movies, hike, sporting event?” and “How many days a week do you usually eat the evening meal with your parents?”), and 4) school attachment (two items: “If I had to move, I would miss my school.” and “I like my school”). Scale descriptions for each confirmatory factor analysis are as follows: attachment to parent (Cronbach’s Alpha = .627), attachment to parental supervision (Cronbach’s Alpha = .95), involvement (Cronbach’s Alpha = .562), and school attachment (Cronbach’s Alpha = .695).

Control variables. Three control variables are included in the analyses: gender, birth place, and city size. To measure gender, the respondents were asked: “Are you male or female?” The item for gender is coded (0 = female, 1 = male). To address birth place, the respondents were asked: “Were you born in this country?” The item for birth place is coded (0 = born in another country, 1 = born in this country). To measure city size, the respondents were asked: “What is your city code?” The item for city size is coded (1 = small, 2 = medium, 3 = large).

Table 1. Descriptive Statistics

Variable	Model 1 (USA)		Model 2 (Venezuela)		Model 3 (Spain)		Model 4 (France)	
	<i>M</i>	<i>SD</i>	<i>M</i>	<i>SD</i>	<i>M</i>	<i>SD</i>	<i>M</i>	<i>SD</i>
Hacking experience	0.03	0.17	0.06	0.25	0.17	0.38	0.05	0.22
LSC	3.28	1.04	2.03	0.89	2.14	1.01	4.46	1.03
ATC to parents	1.41	1.12	1.28	1.06	7.51	1.48	9.65	1.06
ATC to parental supervision	6.24	0.96	1.84	0.87	3.61	0.82	1.36	1.08
ATC to school	4.11	0.99	3.04	0.89	2.11	0.98	3.61	1.14
Involvement	1.72	1.07	1.16	1.11	3.67	0.84	1.10	0.96
Gender	0.52	0.50	0.49	0.50	0.52	0.50	0.50	0.50
Birth place	0.96	0.20	0.99	0.08	0.91	0.28	0.86	0.35
City size	1.80	0.75	2.26	0.96	1.44	0.74	2.54	0.79

Analytic Strategy

Prior to modeling the associations between low self-control, social bonding, and computer hacking offense, the possibilities of multicollinearity among the predictor variables were explored. Tolerance and variance inflation factor statistics demonstrate that multicollinearity is not problematic to execute the current study. Multivariate logistic regression is the proper statistical technique for investigating the effects of low self-control and social bonding on the likelihood of juvenile delinquency for computer hacking due to the nature of the binary dependent variable.

Table 1. Descriptive Statistics (Continued)

Variable	Model 5 (Germany)		Model 6 (Poland)		Model 7 (Hungary)		Model 8 (Russia)	
	<i>M</i>	<i>SD</i>	<i>M</i>	<i>SD</i>	<i>M</i>	<i>SD</i>	<i>M</i>	<i>SD</i>
Hacking experience	0.05	0.22	0.06	0.25	0.05	0.23	0.01	0.13
LSC	1.99	0.92	2.89	0.96	1.74	0.94	2.45	0.98
ATC to parents	6.58	0.93	4.35	1.02	6.02	0.92	4.68	0.94
ATC to parental supervision	1.59	1.10	1.08	1.06	9.95	8.15	1.12	1.01
ATC to school	9.02	0.93	2.71	1.03	2.86	1.04	4.46	0.97
Involvement	1.15	1.00	1.98	1.05	2.38	1.01	3.07	0.97
Gender	0.51	0.50	0.46	0.49	0.51	0.50	0.48	0.50
Birth place	0.98	0.13	0.99	0.10	0.98	0.13	0.94	0.24
City size	3.00	0.00	1.94	0.85	3.00	0.00	2.28	0.96

Table 2. Logistic regression models for juvenile hacking

Predictors	Model 1 (USA)			Model 2 (Venezuela)			Model 3 (Spain)			Model 4 (France)		
	<i>b</i>	S.E	Exp (b)	<i>b</i>	S.E	Exp (b)	<i>b</i>	S.E	Exp (b)	<i>b</i>	S.E	Exp (b)
LSC	0.64***	0.16	1.80	0.42***	0.11	1.52	0.31***	0.07	1.37	0.59***	0.09	1.81
ATC to parents	-0.11	0.11	0.89	-0.07	0.09	0.92	0.07	0.05	1.08	0.01	0.08	1.01
ATC to parental supervision	-0.14	0.14	0.86	-0.24*	0.11	0.78	-0.16*	0.08	0.84	-0.26**	0.08	0.76
ATC to school	-0.18	0.13	0.82	-0.01	0.11	0.98	-0.23**	0.07	0.79	-0.10	0.07	0.89
Involvement	-0.02	0.13	0.97	-0.05	0.09	0.94	-0.21*	0.08	0.81	-0.01	0.09	0.98
Gender	1.07**	0.33	2.90	0.51*	0.21	1.67	0.65***	0.15	1.92	0.85***	0.21	2.36
Birth place	-0.71	0.56	0.48	-1.06	0.70	0.34	1.09**	0.35	2.97	-0.01	0.27	0.99
City size	0.17	0.19	1.10	0.02	0.11	1.02	0.18*	0.09	1.20	0.14	0.12	1.15
Nagelkerke R-Square	.12			.06			.12			.13		
N	2400			2322			1789			3022		

* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$; two-tailed

Results

Table 2 presents the multivariate logistic regression analysis results. As predicted, the results show that self-control and social bonding factors are significant. Specifically, we find support for our expectation that Gottfredson and Hirschi’s low self-control increases the likelihood of computer hacking by 80% (USA: $b = 0.64$, $\text{Exp}(b) = 1.80$), 52% (Venezuela: $b = 0.42$, $\text{Exp}(b) = 1.52$), 37% (Spain: $b = 0.31$, $\text{Exp}(b) = 1.37$), 81% (France: $b = 0.59$, $\text{Exp}(b) = 1.81$), 85% (Germany: $b = 0.61$, $\text{Exp}(b) = 1.85$), 83% (Poland: $b = 0.60$, $\text{Exp}(b) = 1.83$), 86% (Hungary: $b = 0.62$, $\text{Exp}(b) = 1.86$), and 46% (Russia: $b = 0.38$, $\text{Exp}(b) = 1.46$). In other words, juveniles with low self-control are more likely to engage in computer hacking and results show this is the case in all eight countries, across a diverse global sample.

Further, the results provide partial support for our expectation that the elements of social bonding have a link with juvenile computer hacking. First, Table 2 shows that adolescents from Venezuela, Spain, France, Germany, Poland, and Hungary with a strong attachment to parental supervision are less likely to engage in computer hacking. They demonstrate that attachment to parental supervision reduces the likelihood of computer hacking by 22% (Venezuela: $b = -0.24$, $\text{Exp}(b) = 0.78$), 16% (Spain: $b = -0.16$, $\text{Exp}(b) = 0.84$), 24% (France: $b = -0.26$, $\text{Exp}(b) = 0.76$), 86% (Germany: $b = 0.62$, $\text{Exp}(b) =$

Table 2. Logistic regression models for juvenile hacking (Continued)

Predictors	Model 5 (Germany)			Model 6 (Poland)			Model 7 (Hungary)			Model 8 (Russia)		
	<i>b</i>	S.E	Exp (b)	<i>b</i>	S.E	Exp (b)	<i>b</i>	S.E	Exp (b)	<i>b</i>	S.E	Exp (b)
LSC	0.61***	0.09	1.85	0.60***	0.13	1.83	0.62***	0.12	1.86	0.38*	0.16	1.46
ATC to parents	-0.02	0.08	0.97	-0.05	0.11	0.94	-0.13	0.11	0.87	0.17	0.21	1.19
ATC to parental supervision	-0.62**	0.12	1.86	-0.33**	0.10	0.71	-0.36**	0.11	0.69	0.05	0.16	1.05
ATC to school	-0.26**	0.08	0.76	-0.04	0.10	0.96	-0.01	0.10	0.98	-0.33*	0.15	0.71
Involvement	-0.07	0.08	0.92	-0.05	0.11	0.94	-0.12	0.11	0.87	-0.21	0.17	0.81
Gender	1.16**	0.21	3.19	1.76***	0.29	5.83	1.43**	0.27	4.27	2.1	***0.53	8.43
Birth place	0.05	0.31	1.06	1.82	0.42	1.37	0.07	0.66	1.08	-0.35	0.62	0.7
City size	0.04	0.10	1.04	0.01	0.13	1.05	0.08	0.25	1.27	0.31	0.21	1.36
Nagelkerke R-Square	.16			.22			.17			.14		
N	3478			1458			2203			2313		

* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$; two-tailed

1.86), 29% (Poland: $b = -0.33$, $Exp(b) = 0.71$) and 31% (Hungary: $b = -0.36$, $Exp(b) = 0.69$). Second, the findings of this study indicate that adolescents from Spain, Germany, and Russia with strong school attachment are less likely to engage in computer hacking. The results partially support that school attachment attenuates the likelihood of computer hacking by 21% (Spain: $b = -0.23$, $Exp(b) = 0.79$), 24% (Germany: $b = -0.26$, $Exp(b) = 0.76$) and 29% (Russia: $b = -0.33$, $Exp(b) = 0.71$).

Finally, the results indicate that gender is a very strong predictor of juvenile computer hacking. Male adolescents from the eight countries are more likely to engage in computer hacking than female adolescents. Interestingly, the factors of low self-control, attachment to parental supervision, involvement, school attachment, gender, birth place, and city size for Spanish adolescents were strongly associated with computer hacking.

Discussion and Conclusion

The purposes of this study are to make two contributions. First, this study provides an examination of the links between self-control theory, social bonding theory, and juvenile computer hacking. This is supportive of our expectation that social bonding theory has a negative effect on computer hacking, whereas low self-control has a positive effect on computer hacking. Second, this study provides an exploration of the characteristics of juvenile hackers from eight diverse countries around the world. All juvenile hackers from the eight countries tend to have lower levels of self-control, which leads them to be more likely to engage in computer hacking. Also, juvenile hackers from six countries tend to have a strong attachment to parental supervision, which reduces the likelihood of computer hacking. Otherwise, the factors including attachment to parents, involvement, birth place, as well as city size, are not significant predictors of juvenile computer hacking. Despite the environmental differences for each country, surprisingly, the juvenile hackers from the eight countries seem to be influenced by similar factors (i.e., low self-control and attachment to parental supervision) for their hacking behaviors.

Policy Implications

There are clear policy implications to this study. Because computer hacking can potentially cause great damage internationally by negatively impacting infrastructures, voting systems, businesses,

schools, private data, and much more, it is important to find ways to reduce the likelihood that offenders will engage in such behavior. As the results of this study show, increasing self-control and social bonds in juveniles across all cultures can possibly reduce future computer hacking.

Gottfredson and Hirschi (1990) argue that for a person to have high levels of self-control, it must be instilled early in life—ideally before the age of 8-years-old. Furthermore, they argue that effective parenting tactics are the key to self-control, which they say include parents monitoring their children's behavior, recognizing when their children are engaged in the deviant behavior, and providing appropriate and loving guidance to correct that behavior. They support programs designed to provide early education and effective child care, along with programs that target dysfunctional families and seek to improve juvenile supervision. Additionally, Hirschi and Gottfredson (2001) argue for two-parent families to increase monitoring and guidance to children, as well as programs to prevent teen pregnancy. Early childhood intervention programs targeting at-risk children and families (e.g. to teach effective parenting) have proven to be successful in reducing future delinquency in children (Augimeri, Walsh, Donato, Blackman, & Piquero, 2017; Manning, Smith, & Homel, 2013; Olds, 2012; Piquero et al., 2016). Our results indicate that similar programs can also be used to potentially reduce future computer hacking worldwide.

Furthermore, Hirschi and Gottfredson (2001) argue that increased penalties for people with low self-control may not have a significant effect, because offenders with low self-control do not generally consider the long-term consequences of their actions. Instead, they are more impulsive and concerned with short-term rewards. However, increasing supervision or the certainty of being caught in the short-term could reduce offending in those with low self-control, since that would make computer hacking less likely to provide the immediate gratification they seek.

Although not as prevalent, our results also demonstrate that low social bonds can be a predictor of future computer hacking, which also has policy implications. Programs have been developed to increase social bonds in young children with some promising results, although more research must be done (Hawkins, Kosterman, Catalano, Hill, & Abbott, 2005; Brown, Catalano, Fleming, Haggerty, & Abbott, 2005). Many of the same parent training programs that can increase self-control in children can also potentially increase attachment to parents and parent supervision.

Limitations and conclusion

As with any study, there are limitations to these results. First of all, the data is self-report data, which provides both benefits and potential problems. The benefits include uncovering delinquent behavior not found in official data, especially regarding juvenile populations, and assessing self-control and social bond measures. However, we cannot say with absolute certainty that all the juveniles in the sample were truthful or able to accurately self-assess some of the measures, such as those related to self-control. Secondly, although the sample size is relatively large, we do not know if these results are generalizable for most juvenile hackers, especially when exploring it on a worldwide scale. We also cannot say with certainty that these eight countries are representative of the international juvenile hacking population. And, finally, there could be confounding factors not accounted for in this analysis that may better predict juvenile computer hacking. Despite these limitations, this is still a valuable study and contributes to the literature on self-control, social bonds, and juvenile computer hacking.

Computer hacking has become a pervasive criminal issue worldwide, targeting critical infrastructures, voting systems, private data, and academic institutions, potentially costing billions of dollars in damages worldwide. Self-control theory and social bonding theory have frequently been employed to

explain various types of crimes, but rarely to explore computer hacking. This study contributes to the literature by empirically testing the general theory of crime (self-control) and social bonding theory in relation to a sample of 18,985 middle and high school students in eight diverse countries around the world. The results indicate that low self-control is a strong predictor of worldwide juvenile computer hacking, with social bonds also being a predictor, although not as consistently. Therefore, the findings of this study provide strong support for Gottfredson and Hirschi's (1990) self-control theory and partial support of Hirschi's (1969) social bonding theory.

References

- Agnew, R. (1991). A longitudinal test of social control theory and delinquency. *Journal of Research in Crime and Delinquency*, 28(2), 126-156.
- Akers, R. L. (2013). *Criminological theories: Introduction and evaluation*. New York, NY: Oxford Press.
- Augimeri, L. K., Walsh, M., Donato, A., Blackman, A., & Piquero, A. R. (2017). SNAP (Stop Now And Plan): Helping children improve their self-control and externalizing behavior problems. *Journal of Criminal Justice*, 56(18), 43-49.
- Bachmann, M. (2010). The risk propensity and rationality of computer hackers. *International Journal of Cyber Criminology*, 4(1/2), 643-656.
- Bae, S. M. (2017). The influence of strain factors, social control factors, self-control and computer use on adolescent cyber delinquency: Korean National Panel Study. *Children and Youth Services Review*, 78, 74-80.
- Bossler, A. M., & Burruss, G. W. (2012). The general theory of crime and computer hacking: Low self-control hackers? In *Cyber Crime: Concepts, Methodologies, Tools and Applications* (pp. 1499-1527). IGI Global.
- Bossler, A. M., & Holt, T. J. (2010). The effect of self-control on victimization in the cyberworld. *Journal of Criminal Justice*, 38(3), 227-236.
- Bowker, A. L. (1999). Juveniles and computers: Should we be concerned? *Federal Probation*, 63(2), 40-43.
- Brenner, S. W. (2010). *Cybercrime: Criminal threats from cyberspace*. Santa Barbara, CA: ABC-CLIO, LLC.
- Brown, E. C., Catalano, R. F., Fleming, C. B., Haggerty, K. P., & Abbott, R. D. (2005). Adolescent substance use outcomes in the Raising Healthy Children project: a two-part latent growth curve analysis. *Journal of Consulting and Clinical Psychology*, 73(4), 699-710.
- Chan, H. C. O., & Wong, D. S. (2015). The overlap between school bullying perpetration and victimization: Assessing the psychological, familial, and school factors of Chinese adolescents in Hong Kong. *Journal of Child and Family Studies*, 24(11), 3224-3234.
- Choi, K. S. (2015). *Cybercriminology and digital investigation* (p. 340). El Paso, TX: LFB Scholarly Publishing.
- Chua, Y. T., & Holt, T. J. (2016). A cross-national examination of the techniques of neutralization to account for hacking behaviors. *Victims & Offenders*, 11(4), 534-555.

- Cyberthreat real-time map (2018). In Kaspersky Lab. Retrieved from <https://cybermap.kaspersky.com/stats/>.
- DeMarco, J. V. (2001). It's not just fun and war games-Juveniles and computer crime. *United States Attorneys' Bulletin*, 49(3), 48-55.
- Department of Justice, Office of Public Affairs. (2017, March 15). U.S. charges Russian FSB officers and their criminal conspirators for hacking Yahoo and millions of email accounts [Press release]. Retrieved from <https://www.justice.gov/opa/pr/us-charges-russian-fsb-officers-and-their-criminal-conspirators-hacking-yahoo-and-millions>.
- Department of Justice, U.S. Attorney's Office. (2017, March 8). Winchester man sentenced to 24 months for illegally hacking into website and lying to federal agents [Press release]. Retrieved from <https://www.justice.gov/usao-edky/pr/winchester-man-sentenced-24-months-illegally-hacking-website-and-lying-federal-agents>.
- Gentina, E., & Singh, P. (2015). How national culture and parental style affect the process of adolescents' ecological resocialization. *Sustainability*, 7(6), 7581-7603.
- Gottfredson, M. R., & Hirschi, T. (1990). A general theory of crime. Stanford, CA: Stanford University Press.
- Grasmick, H. G., Tittle, C. R., Bursik Jr, R. J., & Arneklev, B. J. (1993). Testing the core empirical implications of Gottfredson and Hirschi's general theory of crime. *Journal of Research in Crime and Delinquency*, 30(1), 5-29.
- Hart, C. O., & Mueller, C. E. (2013). School delinquency and social bond factors: Exploring differences among a national sample of 10th graders. *Psychology in the Schools*, 50(2), 116-133.
- Hawkins, J. D., Kosterman, R., Catalano, R. F., Hill, K. G., & Abbott, R. D. (2005). Promoting adult functioning through social development intervention in childhood: Long-term effects from the Seattle Social Development Project. *Archives of Pediatrics & Adolescent Medicine*, 159(1), 25-31.
- Higgins, G. E. (2006). Gender differences in software piracy: The mediating roles of self-control theory and social learning theory. *Journal of Economic Crime Management*, 4(1), 1-30.
- Higgins, G. E., Fell, B. D., & Wilson, A. L. (2006). Digital piracy: Assessing the contributions of an integrated self-control theory and social learning theory using structural equation modeling. *Criminal Justice Studies*, 19(1), 3-22.
- Higgins, G. E., & Makin, D. A. (2004). Does social learning theory condition the effects of low self-control on college students' software piracy. *Journal of Economic Crime Management*, 2(2), 1-22.
- Higgins, G. E., & Wilson, A. L. (2006). Low self-control, moral beliefs, and social learning theory in university students' intentions to pirate software. *Security Journal*, 19(2), 75-92.
- Higgins, G. E., Wolfe, S. E., & Marcum, C. D. (2008). Digital piracy: An examination of three measurements of self-control. *Deviant Behavior*, 29(5), 440-460.
- Hinduja, S., & Ingram, J. R. (2008). Self-control and ethical beliefs on the social learning of intellectual property theft. *Western Criminology Review*, 9(2), 52-72.
- Hirschi, Travis. (1969). *Causes of delinquency*. Berkeley, CA: University of California Press.

- Hirschi, T., & Gottfredson, M. R. (2001). Self-control theory. *Explaining criminals and crime*, 81-96, Los Angeles, CA: Roxbury.
- Hoffman, L. J., Rosenberg, T., Dodge, R., & Ragsdale, D. (2005). Exploring a national cybersecurity exercise for universities. *IEEE Security & Privacy*, 3(5), 27-33.
- Hollin, C. (2002) Criminological psychology. In: M. Maguire, R. Morgan, and R. Reiner (Eds.), *The Oxford Handbook of Criminology*. Oxford: Oxford University Press.
- Holt, T. J. (2011). Examining the Language of Carders. In *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications* (pp. 127-143). Hershey, NY: IGI Global.
- Holt, T. J., Bossler, A. M., & May, D. C. (2012). Low self-control, deviant peer associations, and juvenile cyberdeviance. *American Journal of Criminal Justice*, 37(3), 378-395.
- Holt, T. J., & Schell, B. H. (Eds.). (2010). *Corporate hacking and technology-driven crime: social dynamics and implications*. Hershey, PA: IGI Global.
- Holt, T. J. (Ed.). (2016). *Cybercrime through an interdisciplinary lens*. New York, NY: Routledge.
- Huebner, A. J., & Betts, S. C. (2002). Exploring the utility of social control theory for youth development: Issues of attachment, involvement, and gender. *Youth & Society*, 34(2), 123-145.
- International Self-Report Delinquency Study (ISRSD). (n.d.). Retrieved from <https://web.northeastern.edu/isrd/isrd2/>.
- Internet Crime Complaint Center (2009) Internet Crime Report. Retrieved from <https://pdf.ic3.gov/2009.IC3Report.pdf>.
- Internet Crime Complaint Center (2010) Internet Crime Report. Retrieved from <https://pdf.ic3.gov/2010.IC3Report.pdf>.
- Internet Crime Complaint Center (2011) Internet Crime Report. Retrieved from <https://pdf.ic3.gov/2011.IC3Report.pdf>.
- Jordan, T., & Taylor, P. (1998). A sociology of hackers. *The Sociological Review*, 46(4), 757-780.
- Kigerl, A. (2016). Cybercrime nation typologies: K-means clustering of countries based on cybercrime rates. *International Journal of Cyber Criminology*, 10(2), 147-169.
- Li, S. D. (2004). The impacts of self-control and social bonds on juvenile delinquency in a national sample of midadolescents. *Deviant Behavior*, 25(4), 351-373.
- Manning, M., Smith, C., & Homel, R. (2013). Valuing developmental crime prevention. *Criminology & Public Policy*, 12(2), 305-332.
- Marcum, C. D., Higgins, G. E., Ricketts, M. L., & Wolfe, S. E. (2014). Hacking in high school: Cybercrime perpetration by juveniles. *Deviant Behavior*, 35(7), 581-591.
- Meldrum, R. C. (2008). Beyond parenting: An examination of the etiology of self-control. *Journal of Criminal Justice*, 36(3), 244-251.
- Menn, J. (2013, July 22). Trillion-dollar global hacking damages estimate called exaggerated. *Reuters*. Retrieved from <https://www.reuters.com/article/us-hacking-estimate-idUSBRE96L0M920130722?feedType=RSS>.

- Mesch, G. S. (2009). Social bonds and Internet pornographic exposure among adolescents. *Journal of Adolescence*, 32(3), 601-618.
- Moon, B., McCluskey, J. D., & McCluskey, C. P. (2010). A general theory of crime and computer crime: An empirical test. *Journal of Criminal Justice*, 38(4), 767-772.
- Muncie, J. (1999). Institutionalized intolerance: Youth justice and the 1998 Crime and Disorder Act. *Critical Social Policy*, 19(2), 147-175.
- Olds, D. (2012). Improving the life chances of vulnerable children and families with prenatal and infancy support of parents: The nurse-family partnership. *Psychosocial Intervention*, 21(2), 129-143.
- Piquero, A. R., Jennings, W. G., Diamond, B., Farrington, D. P., Tremblay, R. E., Welsh, B. C., & Gonzalez, J. M. R. (2016). A meta-analysis update on the effects of early family/parent training programs on antisocial behavior and delinquency. *Journal of Experimental Criminology*, 12(2), 229-248.
- Pratt, T. C., & Cullen, F. T. (2000). The empirical status of Gottfredson and Hirschi's general theory of crime: A meta-analysis. *Criminology*, 38(3), 931-964.
- Real-time visibility into global cyberattacks (2018). Norse. Retrieved from <http://map.norsecorp.com/>.
- Schaefer, B. P., Vito, A. G., Marcum, C. D., Higgins, G. E., & Ricketts, M. L. (2015). Examining adolescent cocaine use with social learning and self-control theories. *Deviant Behavior*, 36(10), 823-833.
- 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.
- Shoemaker, D., & Kennedy, D. B. (2009). Criminal profiling and cyber criminal investigations. In F. Schmalleger & M. Pittaro (Eds.), *Crimes of the Internet* (pp. 439-455). Upper Saddle River, NJ: Pearson Education Inc.
- Simon, D. (2017, October 12). Raising the consequences of hacking American companies. Washington, D.C.: Center for Strategic & International Studies. Retrieved from <https://www.csis.org/analysis/raising-consequences-hacking-american-companies>.
- Steinmetz, K. F. (2015). Craft(y)ness: An ethnographic study of hacking. *The British Journal of Criminology*, 55(1), 125-145.
- Steinmetz, K., & Gerber, J. (2015). "It doesn't have to be this way": Hacker perspectives on privacy. *Social Justice*, 41(3), 29-51.
- Sterling, B. (1994) *The hacker crackdown: Law and disorder on the electronic frontier*. Harmondsworth: Penguin.
- Turgeman-Goldschmidt, O. (2005). Hackers' accounts: Hacking as a social entertainment. *Social Science Computer Review*, 23(1), 8-23.
- Turgeman-Goldschmidt, O. (2008). Meanings that hackers assign to their being a hacker. *International Journal of Cyber Criminology*, 2(2), 382-396.
- Udris, R. (2016). Cyber deviance among adolescents and the role of family, school, and neighborhood: A cross-national study. *International Journal of Cyber Criminology*, 10(2), 127-146.

- Vazsonyi, A. T., Machackova, H., Sevcikova, A., Smahel, D., & Cerna, A. (2012). Cyberbullying in context: Direct and indirect effects by low self-control across 25 European countries. *European Journal of Developmental Psychology, 9*(2), 210-227.
- Veenstra, R., Lindenberg, S., Tinga, F., & Ormel, J. (2010). Truancy in late elementary and early secondary education: The influence of social bonds and self-control-the TRAILS study. *International Journal of Behavioral Development, 34*(4), 302-310.
- Verton, D. (2002). *The hacker diaries*. New York, NY: McGraw-Hill, Inc.
- Wall, D. (2007). *Cybercrime: The transformation of crime in the information age*. Vol. 4. Malden, MA: Polity Press.
- Wiatrowski, M. D., Griswold, D. B., & Roberts, M. K. (1981). Social control theory and delinquency. *American Sociological Review, 46*(5), 525-541.
- Wright, B. R. E., Caspi, A., Moffitt, T. E., & Silva, P. A. (1999). Low self-control, social bonds, and crime: Social causation, social selection, or both?. *Criminology, 37*(3), 479-514.
- Yar, M. (2005). Computer hacking: Just another case of juvenile delinquency?. *The Howard Journal of Crime and Justice, 44*(4), 387-399.
- Yukse, D. A., & Solakoglu, O. (2016). The relative influence of parental attachment, peer attachment, school attachment, and school alienation on delinquency among high school students in Turkey. *Deviant Behavior, 37*(7), 723-747.
- Zhang, L., Young, R., & Prybutok, V. (2008). A Comparison of the Inhibitors of Hacking vs. Shoplifting. In S. Clarke (Ed.), *Evolutionary Concepts in End User Productivity and Performance: Applications for Organizational Progress*. Hershey, PA: IGI Global.