International Journal of Cybersecurity Intelligence & Cybercrime

Volume 3 | Issue 2 Article 2

11-3-2020

The Effects of Self-control on the Cyber Victim-Offender Overlap

Increasingly, the overlap between victims and offenders has received empirical attention with regard to traditional forms of deviance. More recently, the growth of cyber offending has led to a need to examine whether traditional criminological theories can be used to explain these crimes in the same manner as traditional offenses. However, limited attention has been given to victim-offender overlap in cyber-offending. The current study uses a sample of American college students to examine the influence of self-control on cyber offending, cyber victimization, and the cyber victim-offender overlap. The results indicate that low self-control significantly predicts participation in cyber offending as well as cyber victim-offending, but has a weak relationship with cyber victimization. Interestingly, associating with deviant cyber peers was a significant predictor across all models. Results are discussed in the context of the existing literature.

cyber victim-offender overlap, self-control, deviant cyber peers

Recommended Citation

Nodeland, B. (2020). The effects of self-control on the cybercrime victim-offender overlap. International Journal of Cybersecurity Intelligence and Cybercrime, 3(2), 4-24. https://www.doi.org/10.52306/03020220ONXT9834

The Effects of Self-control on the Cyber Victim-Offender Overlap

Brooke Nodeland*, University of North Texas, U.S.A

Keywords; cyber victim-offender overlap, self-control, deviant cyber peers

Abstract:

Increasingly, the overlap between victims and offenders has received empirical attention with regard to traditional forms of deviance. More recently, the growth of cyber offending has led to a need to examine whether traditional criminological theories can be used to explain these crimes in the same manner as traditional offenses. However, limited attention has been given to victim-offender overlap in cyber-offending. The current study uses a sample of American college students to examine the influence of self-control on cyber offending, cyber victimization, and the cyber victim-offender overlap. The results indicate that low self-control significantly predicts participation in cyber offending as well as cyber victim-offending, but has a weak relationship with cyber victimization. Interestingly, associating with deviant cyber peers was a significant predictor across all models. Results are discussed in the context of the existing literature.

Introduction

Americans' comprise one of the largest online markets with nearly 290 million internet users, and 39% of 18-29 year olds reporting they are online almost constantly (Statista, 2018). Such an online presence has led to new opportunities for cyber offending as well as vulnerabilities to cyber victimization. For example, large scale security breaches to corporate records, such as Facebook, Equifax and Capital One, have left personal and identifying information of millions of Americans available to potential cyber offenders (Facts, n.d).

Similarly, there is evidence to suggest that individuals behave online in ways they normally would not in the off-line world (Hinduja & Patchin, 2009; Joinson, 1998; Slonje & Smith, 2008) making them more susceptible to cyber victimization.

*Corresponding author

Brooke Nodeland, Ph.D., Department of Criminal Justice, University of North Texas, 1155 Union Circle #305130, Denton, TX, 76203, U.S.A.

Email: brooke.nodeland@unt.edu

Suler (2004), for example, describes an online disinhibition effect characterized by diminished internal censorship online resulting from a variety of factors, including a high sense of perceived anonymity and a lower level of social control online making individuals more likely to disclose detailed personal information (Spears, Slee, Owens, & Johnson, 2009). The continual growth in Internet usage and information sharing has been coupled with increased empirical attention to the theoretical predictors of cyber offending and cyber victimization to explore the relevance of traditional criminological theories to these new types of behaviors. Specifically, Gottfredson and Hirschi's (1990) self-control theory has received considerable attention with regard to cyber offending (e.g. Donner, Marcum, Jennings, Higgins, & Banfield, 2014; Evans, Cullen, Burton, Dunaway, & Benson, 1997; Gibson & Wright, 2001; Higgins 2007; Higgins, Wolfe, & Marcum, 2008; Malin & Fowers, 2009; Moon, McCluskey, & McCluskey, 2010) and, increasingly, cyber victimization (Bossler & Holt, 2010; Hinduja & Patchin, 2008; Holt, Bossler, Malinski, & May, 2016; Ngo & Paternoster, 2011; Reyns, Burek, Henson, & Fisher, 2013; Reyns, Fisher, Bossler, & Holt, 2019).

The link between self-control, cyber offending, and cyber victimization, generally reflects the established impact of self-control on more traditional forms of offending and victimization in that low self-control is consistently found to predict both victimization and participation in deviant behavior. While Gottfredson and Hirschi's (1990) theory was not designed to account for both victimization and offending, they do contend that victims and offenders share many social and personal characteristics, such as low self-control, which may increase individual likelihood of being involved in both offending and victimization (Schreck, 1999). In fact, there is mounting evidence that many offenders are more likely to be crime victims and that crime victims are at times engaged in some types of offending (e.g., Kerstens & Jansen, 2016; Kranenbarg, Holt, & van Gelder, 2019). This victim-offender overlap for traditional crime types has received a considerable amount of attention showing that victims are likely to commit criminal acts, and that offenders have a high likelihood of being victims themselves (e.g., Berg et al., 2012; Averdijk, Gelder, Eisner, & Ribeaud, 2016; Hay & Evans, 2006; Lauritsen & Laub, 2007; Lauritsen et al., 1991; Ousey et al., 2011; Schreck et al., 2008), while the cyber victim-offender overlap has only begun to be explored (Kerstens & Jansen, 2016; Kranenbarg et al., 2019).

Empirical attention to the victim-offender overlap in cyber deviance has primarily focused on cyberbullying (e.g. Craig et al., 2009; Hinduja & Patchin, 2009; Vandebosch & Van Cleemput, 2009; Ybarra & Mitchell, 2004), whereas only two studies have specifically examined the cyber victim-offender overlap for cybercrimes, including general cyber offending (Weulen Kranenbarg, Holt, & van Gelder, 2019) and financial cybercrimes (Kerstens & Jansen, 2016). The current study uses a sample of American college students to examine the role of low self-control in the cyber victim-offender overlap. Specifically, the study uses a combined measure of several types of cyber offending to determine the factors that predict cyber offending, cyber victimization, and cyber victim-offending.

Self-Control Theory

A General Theory of Crime describes self-control theory and explains involvement in criminal behavior as a by-product of low self-control, or propensity for crime (Gottfredson & Hirschi 1990). Self-control shapes how individual's respond to criminal opportunities either through deviance or refrainment from criminal behavior.

The general theory explains both conforming and deviant behavior in that the presence of a developed sense of self-control prevents involvement in deviance in a similar manner as an underdeveloped sense of self-control, or low self-control, allows an individual to view criminal behavior as pleasurable. The theory further identifies several specific characteristics of low self-control, including: impulsivity, insensitivity, risk taking, shortsightedness, minimal tolerance for frustration, a tendency to respond to conflict through physical means, and a preference for simple tasks, however, Grasmick, Tittle, Bursik, and Arneklev (1993) operationalized these characteristics into impulsivity, simple tasks, risk seeking, physical activities, self-centered, and temper. These characteristics influence individual behavior by affecting their ability to control impulses, manage risk tasking, exact predictability on an individual's life, perform complex thought processes, and exercise control over individual emotions. The authors suggest that individuals are inherently motivated to engage in crime because they naturally view crime as pleasurable or in their own self-interest (Grasmick et al., 1993). Rather, crime satisfies individual desires for immediate or short-term gratification with the reward for criminal behavior following shortly after the commission of an act.

Gottfredson and Hirschi's (1990) self-control theory has received considerable empirical attention and has been used to explain involvement in a variety of traditional offenses (e.g. Pratt & Cullen, 2000; Vazsonyi, Mikuška, & Kelley, 2017), white-collar and cyber offenses (Donner, Marcum, Jennings, Higgins, & Banfield, 2014; Evans et al., 1997; Gibson & Wright, 2001), and, most recently, victimization, including cyber victimization (see Pratt, Turanovic, Fox, & Wright, 2014).

Gottfredson and Hirschi (1990) contend that offending and victimization are highly correlated because both are the result of inadequate levels of self-control. Piquero, MacDonald, Dobrin, Daigle, and Cullen (2005) argue that if self-control predicts offending, and offenders and victims possess similar personal characteristics, then it is reasonable to expect that self-control predicts victimization. This suggests that low self-control may make an individual both susceptible to the temptations of crime and more vulnerable to victimization. Specifically, the same characteristics of low self-control (e.g. shortsightedness, insensitivity, impatience, risk-taking) that increase the odds of committing crime also increase the likelihood of victimization (Bossler & Holt, 2010). Rather, individuals with low self-control make impulsive decisions which increases their vulnerability and exposure to offender populations thereby also increasing their risk of victimization (Bossler & Holt, 2010). For example, individuals with low self-control may place themselves in risky situations and possibly act in an unadvised manner (Bossler & Holt, 2010) indicating that this behavior not only increases crime opportunities, but also increases victimization (Forde & Kennedy, 1997). Schreck (1999) further suggests that the effect of self-control on victimization may be mediated by offending measures, or that self-control influences victimization only if it places individuals closer in proximity to offenders. Piquero, MacDonald, Dobrin, Daigle, and Cullen (2005) further suggest that if self-control predicts offending, and if offenders and victims possess similar personal characteristics, then it is reasonable to expect that self-control predicts victimization. The theory seems to suggest that low self-control renders an individual both susceptible to the temptations of crime and more vulnerable to victimization.

More recently, this empirical examination of traditional criminological theories has been extended to online behaviors. Further, a number of studies have found an empirical link between traditional criminological theories and cybercrime offending as a risk factor for cybercrime victimization (e.g., Bossler & Holt 2009, 2010; Choi 2008; Holt & Copes, 2010; Wolfe, Higgins, & Marcum, 2008). While others have found that cybercrime victimization is a risk factor for cybercrime offending (e.g., Bossler & Holt, 2009; Ngo & Paternoster, 2011).

Of these theories, the general theory has received a considerable amount of attention with regard to cybercrime and there is some evidence of shared risk factors for cybercrime offending and cybercrime victimization in the literature.

Cyber Offending

The extension of self-control theory to non-traditional crime types was discussed by Gottfredson and Hirschi (1990) in their explanation of white-collar crime. Specifically, they argue that individuals who engage in criminal behavior share common characteristics, such as low self-control, and suggest that their theory be extended to other types of offenders including white collar criminals. Following this same logic, the theory may be extended to explain participation in cybercrime offending as well. For example, digital pirates demonstrate the characteristics of low self-control in their inability to delay the gratification of waiting for the official release of digital media (Malin & Fowers, 2009; Moon et al., 2010; Nodeland & Morris, 2020b). The relationship between self-control and cyber offending has been well tested with findings suggesting generally consistent support for the link between low self-control and cyber offending (e.g. Holt & Bossler, 2014). For example, Foster (2004) established a link between self-control and cyber offending in his examination of undergraduate students finding moderate direct and positive support for the relationship between low self-control and opportunity on cyber offending. Moon and colleagues (2010) further found support for the link between self-control and digital piracy in their examination of a sample of 2,751 Korean youth. Their findings indicate the applicability of low self-control in explaining the illegal downloading of software and the illegal use of others' personal identification online. More recently Donner and colleagues (2014) utilized a sample of 488 U.S. undergraduate students to examine the theory's generality hypothesis and found that low self-control is related to online deviance in general as well as cyber offenses beyond digital piracy including posting hurtful information online, email/IM harassment, excluding someone online, hacking, and misusing someone else's personal information.

Deviant peer associations have been found to be a significant predictor of participation in cyber offending that further explains the relationship between self-control and cyber offending. Specifically, associating with deviant peers can be applied to cyber offending as commission of these offenses requires a unique skill set individuals generally acquire through personal interactions or experiences that they do not naturally possess (Skinner & Fream 1997). Further, the nature of the internet allows users to establish virtual peer relationships with individuals with whom they have no face-to-face relationship, but with whom they associate only in an online environment (Warr 2002), expanding the possible pool of influences from whom they learn criminal behaviors themselves. A variety of studies of cyber offending and technology illustrate the importance of deviant peers on offending behavior related to computer hacking (Bachmann 2010; Holt 2007, 2009; Jordan & Taylor 1998), digital piracy (Cooper & Harrison 2001; Holt & Copes 2010), and general cyber offending (Nodeland & Morris 2020a).

Cyber Victimization

Self-control theory has also been used to explain victimization. There is mounting evidence to suggest that offenders and victims share many of the same characteristics and that the theory can logically be extended to explain traditional victimization in a similar manner as offending (Holtfreter et al., 2008; Piquero et al., 2005; Schreck, 1999; Schreck, Fisher, & Miller, 2006; Schreck, Wright, & Miller, 2002; Stewart et al,. 2004).

As the relationship between low self-control and cyber offending has been established in the literature, it is plausible that the theory may then be able to explain cybercrime victimization as well. However, Bossler and Holt's (2010) study of self-control on various types of cybercrime victimization found a weak relationship between self-control and certain types of cyber victimization, but no direct effect on victimization after controlling for offending measures. Their findings may suggest that individual characteristics, such as low self-control or choice, are less important in understanding certain types of cybercrime victimization than others. This may be even more likely since some types of cybercrime victimization, such as malicious software infections or credit card number theft, can occur through no fault of the victim (Bossler & Holt, 2010). Rather, some forms of cyber victimization occur with little or no direct interaction between victims and offenders (e.g. Chien, 2003; Taylor et al., 2006; Bossler & Holt, 2010), and may be completely random suggesting that an individual's level of self-control may not be the most important predictor in determining cybercrime victimization.

Studies examining the effect of low self-control and other theoretical constructs, such as deviant peer associations, have provided further insight into this relationship. Specifically, associating with deviant peers is a consistent predictor of traditional forms of victimization and has been found to be related to cybercrime victimization as well. Deviant cyber peer association places individuals in closer proximity to cybercrime offenders increasing their likelihood of cyber victimization (Bossler & Holt, 2009, 2010; Bossler, Holt, & May, 2012; Reyns & Henson, 2016).

For example, Bossler and Holt (2010) found deviant peer associations to significantly predict cyber victimization across multiple cybercrime types. More specifically, college students indicating higher numbers of deviant cyber peer associations were more likely to report cyber victimization across cybercrime types including someone obtaining their password to access their computer files, someone modifying their information on their computer without their permission, being infected by a virus, someone electronically obtaining their credit card number without their knowledge or permission, and someone harassing them in a chatroom or instant message. Their finding extends the traditional criminological literature that indicates associating with delinquent peer's places individuals in risky situations where victimization can occur (Bossler & Holt, 2010; Lauritsen, Laub, & Sampson, 1992).

The Cyber Victim-Offender Overlap

To date, empirical attention has generally focused on cybercrime offending and cybercrime victimization as separate constructs, including in the self-control literature. While the literature surrounding traditional criminal behavior provides some evidence that offending has a direct effect on victimization and that victimization has a direct effect on offending (e.g. Berg & Felson, 2016; Jennings, Piquero, & Reingle, 2012; Lauritsen & Laub, 2007), not all offenders are at risk of victimization and not all victims engage in criminal behavior (Weulen Kranenbarg et al., 2019). Given these findings, it has become increasingly important to consider offenders-only, victims-only, and victim-offenders separately in order to identify differences in underlying risk factors (e.g. Shcreck, Stewart, & Osgood, 2008, Van Gelder et al., 2015; Weulen Kranenbarg et al., 2019).

Prior studies examining the cybercrime victim-offender overlap are sparse; in fact, only two studies to date have examined this relationship. The first study, by Kerstens and Jansen (2016), utilized a sample of sample of Dutch youth aged 10-18 (n = 6,299) to examine the victim-perpetrator overlap for financial cyber offenses including auction fraud, virtual theft, and identity fraud. The results of multinomial regression indicate a positive and significant relationship between low self-control and online disinhibition with both financial cyber offense victimization and perpetration.

Their findings further demonstrate that the overlap between financial cybercrime victimization and perpetration is partially explained by retaliation, low self-control and online disinhibition. More recently Weulen Kranenbarg, Holt and van Gelder (2019) used a sample of 535 high risk Dutch adult (18+) suspects of cybercrime and traditional crime to compare victimization, offending, and victimization-offending between cybercrime and traditional crime. With regard to cybercrime, their results indicate a considerable victim-offender overlap with correlates such as low self-control and routine activities partly explaining differences in victimization, offending, and victimization-offending.

The findings from both Kerstens and Jansen (2016) and Weulen Kranenbarg and colleagues (2019) indicate that low self-control at least partially explains the victim-offender overlap in financial cyber offending as well as a variety of other cybercrimes such as malware, hacking, phishing, etc. Informed by these two studies, the current study examines the cyber victim-offender overlap using a sample of undergraduate students in the U.S to provide further clarification of the impact of low self-control on participation in cyber offending and cyber victimization. Specifically, this study examines the impact of low self-control on the victim-offender overlap for a variety of general cyber offending behaviors. Three research questions are assessed to explore this relationship. (1) Does low self-control increase the odds of participating in cyber offending? (2) Does low self-control increase the odds of cyber victimization? (3) Does low self-control significantly increase the odds of both engaging in cyber offending and experiencing cybercrime victimization? Based on the previous research, it is expected that low self-control will significantly increase the odds of cyber offending, cyber victimization, as well as the cyber victim-offender overlap.

Methods and Sampling

Data for the current study were obtained via an original data collection effort during the spring 2018 semester at a midsize suburban public university in the southern part of the United States. Upon approval from the university's institutional review board, an anonymous survey link was sent to all registered students in a single college, or one group of related departments reporting to the same dean, at the university. Specifically, an email was sent to all registered students university email accounts requesting participation in the online survey. The survey was sent a single time and left open for two weeks. Due to university restrictions, no follow-up emails were sent. Respondents were advised that their responses were anonymous and voluntary and that they could cease participation in the study at any time. No identifying information was collected from respondents. Emails were sent to approximately 2600 students in the college with 598 student respondents for a response rate of roughly 23%. Seventy eight cases were removed due to missing data or Mahalanobis Distance scores exceeding the 0.01 cutoff (Tabachnick and Fidell, 2007) resulting in a final convenience sample of n=517. The final sample was comprised of 335 cyber offenders, 381 cyber victims, and 240 cyber victim-offenders. Prevalence rates were higher among respondents in the cyber-victim group in comparison to the cyber-offender group in almost all areas (see variable description below).

Dependent Variables

The first dependent variable, c*yber offending*, was measured by asking respondents a series of questions about their deviant behaviors online. The items included in this outcome measure were derived from measures used in previous cyber offending studies and include a range of cyber offending behaviors (e.g. Skinner & Fream, 1999; Nodeland & Morris, 2020a).

Respondents were asked to report the number of times they had participated in the following activities within the past year: posted hurtful information about someone through social media (9 respondents), purposefully excluded someone from an online community (64 respondents), threatened or harassed someone through e-mail or instant messaging (9 respondents), threatened or harassed someone through online gaming (13 respondents), posted nude or sexually explicit images of someone online without their permission (2 respondents), committed any type of hacking by gaining access to unauthorized areas of the Internet or another person's secure account (11 respondents), used someone else's personal information (e.g. credit card) without their permission to obtain goods or services through the Internet (1 respondents), illegally downloaded copyright protected files (77 respondents), or illegally uploaded copyright protected files (17 respondents). These items were then summed and dichotomized where the final measure represents 1 = cyber offending within the past year and 0 = no cyber offending within the past year. The final variable consisted of 55% of respondents reporting participation in some form of cyber offending in the past year and 45% of respondents reporting no participation in cyber offending in the past year.

The next dependent variable, c*yber victimization*, was measured by asking respondents a series of questions about their victimization online. The items included in this measure reflect those used in the cyber offending variable but relate to cyber victimization as opposed to offending. This outcome variable includes only items that line up with those included in the cyber offending outcome measure described above. Specifically, respondents were asked how many times they had experienced the following types of cyber victimization within the past year: someone posted hurtful information about them through social media (61 respondents), been purposefully excluded from an online community (47 respondents), been threatened or harassed through email (69 respondents), been threatened or harassed through online gaming (8 respondents), had someone post nude or sexually explicit images of them online without their permission (4 respondents), had someone attempt to gain access to their personal information online (such as their email, social media, etc.) (126 respondents), or had someone use their personal information, e.g. credit card, without their permission to obtain goods or services through the Internet (100 respondents). These items were summed and dichotomized where the final measure represents 1 = cyber victimization within the past year and 0 = no cyber victimization within the past year. The final variable consisted of 69% of respondents reporting some form of cyber victimization in the past year and 31% of respondents reporting no cyber victimization in the past year.

The final dependent variables, c*yber victim-offender* is a combined measure of the variables described above. The dichotomous measures of cyber offender and cyber victimization were summed and then dichotomized where the final variable reflected 1 = both cyber offending and cyber victimization within the past year and 0 = was not both a participant in and victim of cyber offending in the past year. The final variable consisted of 44% of respondents reporting both cyber offending and cyber victimization in the past year, while the majority of respondents, 56%, did not report both cyber offending and cyber victimization in the past year.

Independent Variables

Self-control. The self-control measure used in this study is derived from Tangey, Baumeister, and Boone's (2004) scale and shows good internal consistency and retest reliability. This condensed self-control scale is well cited and is designed to reflect the respondents established level of self-control (Morris & Higgins, 2009; Nodeland & Morris, 2020) while asking respondents fewer questions to measure the same concept as other measures of self-control.

As such, respondents were asked a series of 13 questions measuring their established level of self-control. Specifically, the scale measured higher levels of self-control and were reported on a 1-5 scale where 1=not at all and 5=very much. These items included (1) I am good at resisting temptation, (2) I refuse things that are bad for me, (3) people would say that I have iron self-discipline, and (4) I am able to work effectively toward long-term goals. Additional self-control indicators were included in the scale were reported on a 1-5 scale where 1=not at all and 5=very much but were reverse coded prior to inclusion in the self-control for analysis. These items include (1) I have a hard time breaking bad habits, (2) I am lazy, (3) I say inappropriate things, (4) I do certain things that are bad for me if they are fun, (5) I wish I had more self-discipline, (6) pleasure and fun sometimes keep me from getting work done, (7) I have trouble concentrating, (8) sometimes I can't stop myself from doing something even if I know it is wrong, and (9) I often act without thinking through all the alternatives. The result was a standardized single factor measuring the concept of self-control where higher values indicated higher levels of self-control and explaining 93% of the variance (α=.85).

Deviant peers. The independent variable, *deviant peers*, is a summed measure of 6 items measuring respondent peers' involvement in a variety of deviant cyber behaviors. Items included in this measure are based on peer behavior available in the data. Specifically, respondents were asked how many of their three closest friends engaged in the following behaviors in the past year: posted hurtful information about someone through social media, threatened or harassed someone online, posted nude or explicit images of someone online without his/her permission, committed any type of hacking by gaining access to unauthorized areas of the Internet or another person's secure account, helped distribute malicious software, or used someone else's personal information, e.g. credit card, without his/her permission to obtain goods or services through the Internet. These items were summed and then dichotomized to create the final variable where 1 = deviant cyber peers and 0 = no deviant cyber peers. Approximately 16% of respondents reported having at least 1 deviant cyber peer while 84% reported no deviant cyber peers.

Control variables. Several control variables were selected based on their significance in previous studies of cyber offending and victimization. Individual characteristics such as gender (e.g. Donner, 2016; Hollinger, 1993), age (e.g. Hollinger, 1993; Seale, Polakowski, & Schneider, 1998; Sims, Cheng, & Teegen, 1996; Solomon & O'Brien, 1990), hours spent online (e.g. Donner, 2016; Holt & Turner, 2012; Pratt et al., 2010), and level of computer knowledge (e.g. Eining & Christensen, 1991; Hinduja, 2001; Holt & Bossler, 2013; Malin & Fowers, 2009; Sims et al., 1996) are associated with cyber offending and victimization.

The current analysis accounts for gender and race as dichotomous variables where 0=female, 1=male and 0=non-White, 1=White. The analyses were run using dichotomous measures of White/non-White, Black/non-Black, and Hispanic/non-Hispanic. There were no changes in the outcome of the models based on any category of race that was included. Just over half of the sample, 54%, were female, and the majority of the sample, 64%, were White. Respondent age is a continuous variable and is based on the respondent's age (in years) at the time of data collection. The average age of the sample was 28. Hours spent online is an interval level variable where 1=0-6 hours per day spent online, 2=7-12 hours per day spent online, 3=13-18 hours per day spent online and 4= 19-24 hours per day spent online. The average amount of time spent online each day was approximately 6 hours.

Finally, respondent's computer skill level was measured by asking respondents to self-report their skill level by choosing one of the following options: 1 = I am uncomfortable using computers, 2 = I can "surf the 'net", use common software, but not fix my computer problems, 3 = I can use a variety of software and fix some of my computer problems, 4 = I can use a variety of operating systems and fix most computer problems I have, or 5 = I am comfortable manipulating or writing computer programming (e.g. Holt & Morris 2009; Miller & Morris 2016). For analysis, this variable was dichotomized to reflect low and high skill level where 0=novice and 1=expert. In the final sample, 83% of respondents were considered novice computer users and 17% were categorized as expert.

Table 1. Descriptive statistics

	N	*%*	*Mean*	*SD*	*Min*	*Max*
Self-control			4.88	1.04	1.6	7.6
Cyber offenders	335	55%			0	1
Cyber victims	381	69%			0	1
Cyber victim-offenders	240	44%			0	1
Deviant cyber peers	83	15%			0	1
Gender (male)	296	55%				
Race						
White	336	65%				
Black or African American	53	10%				
Asian	6	1%				
American Indian or Pacific Islander	27	5%				
Hispanic/Non-white	79	15%				
Other	19	4%				
Age			28.23	10.12	18	65
Hours per day spent online			6.15	3.77	0	24
1-6 hours	417	66%				
7-12 hours	180	29%				
13-18 hours	23	4%				
19-24 hours	9	1%				
Skill level with computers			2.88	0.84	1	5
Novice	521	83%				
Expert	108	17%				

Analytical Strategy

The current study utilizes 3 separate models to examine the relationship between self-control and cyber offending, self-control and cyber victimization, and a self-control and cyber victim-offenders. Stata 15 was used to run a series of logistic regression's to analyze these data based on the use of three separate dichotomous dependent variables. Results are presented in odds ratios and are accompanied by Cragg & Uhler's R2 assessing model fit as well as the cases correctly classified. Variables were checked for multi-collinearity and none of them had VIF scores above 10 individually and the overall mean VIF did not exceed 6 (O'Brien, 2007). Three models were analyzed to examine the impact of self-control on cyber offending, cyber victimization, and cyber victim-offenders. Specifically, Model 1 uses logistic regression to examine the impact of self-control and other factors on cyber offending. Model 2 uses logistic regression to examine the impact of self-control and other factors on cyber victimization. Model 3 uses logistic regression to examine the impact of self-control and other factors on cyber victim-offenders.

Results

The current study used three logistic regression models to examine the relationship between self-control and cyber offenders, cyber victims, and cyber victim-offenders. Logistic regression was utilized due to the dichotomous nature of the dependent variables. Self-control was incorporated into three separate models to determine if there are differences in theoretical predictors for cyber offenders, cyber victims, and cyber victim-offenders. These analyses examined the odds of engaging in cyber deviance, the odds of being a victim of cyber deviance, and the odds of both engaging in cyber deviance and being a cyber-victim. Appropriate measures of model fit are addressed for each model. Unless otherwise noted, a $p<.05$ level of significance was utilized.

Table 2 provides the results of the logistic regression models. Model 1 provides the results of the logistic model examining the relationship between self-control and cyber offending. Fit statistics indicate that 63.64% of cases were correctly classified for each of these models, and pseudo R^2 measures suggest reasonable fit .15 (Cragg & Uhler's R^2). There were three significant predictors of participation in cyber offending including low self-control, having at least one deviant cyber peer, and being White. Rather, as self-control increases, the odds of engaging in cyber offending decrease by 44%. Associating with at least one peer who has engaged in cyber offending in the past 12 months increases the odds of participation in cyber offending by 49%. And being White increases the odds of participation in cyber offending by 55%.

Model 2 provides the results of the logistic model examining the relationship between self-control and cyber victimization. Fit statistics indicate that 67.64% of cases were correctly classified for each of these models, and pseudo R^2 measures suggest reasonable fit .10 (Cragg & Uhler's R^2). The lower R^2 for the victims only model in comparison to the offender model is likely a result of the predictor variables used in these models. The predictor variables are commonly associated with cyber offending variables and would therefore be better at predicting offending models.

Table 2. Logistic regression results

	Model 1 Cyber offenders		Model 2 Cyber victims		Model 3 Cyber victim-offenders	
	OR	SE	OR	SE	OR	SE
Low self-control	0.5641	0.05681***	0.8264	0.0852[1]	0.6303	0.0624***
Deviant cyber peers	1.4923	0.2093**	1.8404	0.3229***	1.6359	0.2188***
Hours per day spent online	1.0196	0.1589	1.1965	0.2054	1.1210	0.1733
Skill level with computers	1.4121	0.3750	1.4175	0.4139	1.4823	0.3845
Age	0.9943	0.0099	1.0204	0.0113	0.9961	0.0101
Race	1.5507	0.3107**	0.4519***	0.4519***	1.7938	0.3647**
Gender	0.8312	0.1619	0.2949	0.2949	1.0470	0.2041
Constant	15.7728	9.3302	0.6708	0.6708	3.8100	2.1636
N	517		516		516	
Chi2	61.83		37.90		55.18	
Cases correctly classified	63.64%		67.64%		65.50%	
Cragg & Uhler's R2	0.15		0.10		0.13	

* p<0.05, ** p<0.01, *** p<0.001

[1]significant at p=0.06

It also indicates that the inclusion of additional variables specified for victimization may increase model fit and be important in future examinations of the cyber victim-offender overlap. While the odds ratio for low self-control was in the expected direction, its effect on cyber victimization was only marginally significant in this model (p=.06). Similar to the cyber offender model, two other predictors were significant in this model, deviant cyber peers and race. Specifically, associating with at least one deviant cyber peer increased the odds of experiencing cyber victimization by 84% and being White increased the odds of cyber victimization by 117%.

Model 3 provides the results of the logistic regression model examining the relationship between self-control and cyber victim-offenders, or those who reported both participation in and experiencing victimization by cyber offending in the past year. Fit statistics indicate that approximately 65.50% of cases were correctly classified for this model, and pseudo R^2 measures suggest reasonable fit .13 (Cragg & Uhler's R^2).

There were three significant predictors in this model. Specifically, as self-control increases, the odds of engaging in cyber offending decrease by 36%, having at least one deviant cyber peer increases the odds of being a cyber victim-offender by 63%, and being White significantly increases the odds of being a cyber victim-offender by 79%.

Discussion and Conclusions

The purpose of this study was to examine the impact of low self-control on the cyber victim-offender overlap among a sample of American college students. The study uses logistic regression to examine the relationship between low self-control on cyber offending and cyber victimization separately as well as on the cyber victim-offending overlap. Findings from the current study are in line with previous studies that provide support for the impact of low self-control on cyber offending (e.g. Boillot Fansher, 2017; Bossler & Holt, 2010; Higgins et al., 2007; Holt et al., 2012; Marcum et al., 2014; Reyns, 2019), and the cyber victim-offender overlap, conversely, there was only marginal significance (p=0.06) on cyber victimization. These findings suggest low self-control among cyber offenders is likely driving the influence on cyber victim-offenders, and that this individual level predictor should be further explored with regard to cyber victimization. While there has been some support in the previous literature for the impact of low self-control on certain types of cyber victimization (Bossler & Holt, 2010), the use of a combined measure of cyber victimization in the current study could provide partial explanation for these results. For example, while several forms of cyber victimization may have occurred in personal relationships or with knowledge of the offender (e.g. someone posting hurtful information about them through social media, being threatened or harassed through email, etc.), others may have occurred with little or no direct interaction between victims and offenders (e.g. someone using their personal information such as a credit card number to make purchases online).

The relationship between low self-control and the cyber victim-offender overlap is in line with previous research (Kerstens & Jansen, 2016; Weulen Kranenbarg et al., 2019). Both of these studies found a strong influence of low self-control on the cyber victim-offender overall looking at more specific forms of cyber behaviors. Associating with at least one deviant cyber peer appears to significantly influence the odds of engaging in cyber offending, being the victim of cyber deviance, and of both engaging in and being the victim of cyber deviance.

This suggests that while low self-control is a significant correlate for engaging in cyber offending, the role of other theoretical perspectives warrant further examination. Deviant cyber peer association was significant across models which possibly lends support to at least two theoretical arguments. First, deviant cyber peers appear to play a role in the cyber victim-offender overlap in a similar manner as traditional peers to the traditional victim-offender overlap. While a variety of studies have established a mediating relationship between low self-control and associating the deviant cyber peers with regard to cyber offending (e.g. Holt, Bossler, & May, 2012; Nodeland & Morris, 2020a), the role of these two theories in examining the victim-offender overlap in cyber deviance remains underexplored. Further, associating with deviant cyber peers may expose cyber victims to additional vulnerability due the types of information they share with their deviant cyber peers or the types of activities they engage in online. While previous studies have considered other theoretical predictors including routine activities (Weulen Kranenbarg et al., 2019) and online disinhibition (Kerstens & Jansen, 2016), additional examination of other theoretical predictors in addition to self-control and the victim-offender overlap is necessary.

First, skill level with computers was not significant in any of the models. While previous studies have found a significant relationship between skill level and cyber offending (Eining & Christensen, 1991; Hinduja, 2001; Malin & Fowers, 2009; Sims et al., 1996), findings from this study suggest that individual skill level has little impact on cyber offending or cyber victimization.

While it would seem likely that more skilled individuals would be better equipped to protect themselves from cyber victimization, it may instead be that cyber victimization is random in nature and appears to impact both skilled and unskilled computer users. Also of interest, is that traditional correlates of cyber offending, including age and gender, were not significant in any of the models while race was significant across all models. Being White increased the odds of cyber offending, cyber victimization, and cyber victim-offending by at least 50% across models. Further examination of differences in predictors between racial groups was not possible due to the limited participation of different groups, however, this finding does provide another area for future consideration.

This study uses a sample of American college students to add to the discussion of the impact of self-control on cyber offenders, cyber victims and the cyber victim-offender overlap. While there are several interesting findings, the study has several limitations that should be considered in future research. First, respondents in this sample are comprised of college students at a single university and may not be generalizable to a more diverse or general population. Previous studies have utilized college students to examine cyber offending extensively (e.g. Hinduja & Ingram, 2008, 2009; Morris & Higgins, 2009, 2010; Holt, Burruss, & Bossler, 2010; Nodeland & Morris, 2020b; Reyns, 2019; Skinner & Fream, 1997; Wolfe et al., 2009), with more recent limited utilization for cyber victimization (e.g. Bossler & Holt, 2010; Reyns et al., 2018). College students who have grown up with personal technologies, such as those in current college samples, may differ from younger individuals and older generations with regard to their behavior online and risk of victimization. For example, college students may be more likely to take protective measures of their personal information in comparison to younger individuals. Younger individuals have greater access to personal technologies than ever before while also possessing more limited experience or knowledge of how their information sharing online may affect them. Further examination of more general populations would provide greater insight into the influence of theoretical predictors on the cyber victim-offender overlap.

Also, while cyber offenders are in a position to self-report their own behavior, cyber victims may not know they have been victimized and therefore would not be able to self-report their victimization (see Holt & Bossler, 2014). Cyber victims may lack the technical skills to identify a problem and may not become aware of their victimization until years later if at all. For example, cyber victims may only become aware of hacking victimization after their information has been removed or corrupted (Wall, 2007). A lack of general knowledge and underreporting makes it more difficult to develop a complete understanding of the correlates of cyber victimization. Additional research targeting known cyber victims may provide more insight into the theoretical predictors of cyber victimization and the cyber victim-offender overlap.

This study is also limited in its examination of theoretical influences on the cyber victim-offender overlap. Data were initially collected to examine the influence of self-control on a variety of cyber offending behaviors. The data contain less information on types of cyber victimization or other theoretical explanations for cyber offending, such as social learning theory (Akers, 1973). The findings from this study indicate the importance of deviant peers in the victim-offender overlap suggesting future studies should incorporate full measures of other theoretical predictors of the cyber victim-offender overlap.

For example, peer effects in the cyber victim-offender overlap could be directly assessed by examining a full social learning model that incorporates measures of the influence of both traditional and virtual peers (Miller & Morris, 2016).

Despite these limitations, there remain opportunities for both proactive and reactive policy recommendations in the future. The significance of deviant peer associations supports a continued effort to incorporate learning considerations into policies targeting reductions in cyber offending and cyber victimization. Reducing the occurrence of cyber offending would likely have the effect of reducing the occurrence of cyber victimization. If there are less offenders, in theory, there should also be fewer victims. Educational approaches aimed and reducing at preventing cyber offending include publicizing the likelihood of apprehension and conviction for cyber offending as well as the types of sentences that typically accompany these offenses. Increased awareness of the chances of getting caught and what might happen when caught may influence the way that potential offenders think about cyber offending and influence the likeliness of offending. Deterrence programs addressing increased responses to cyber offending, including arrest and prosecution, may also reduce participation. Educational programs for victims may include campaigns similar to "Lock your car, Hide your keys", but with regard to protecting oneself online. Providing the public with simple recommendations to protect themselves online may both reduce their likelihood of victimization and make it more difficult for cyber offenders to engage in this behavior as potential victims make more effort to protect themselves online.

In conclusion, this paper sought to provide further information on the influence of self-control on the cyber victim-offender overlap. Low self-control was found to have a significant relationship with cyber offending participation as well as cyber victim-offending, while only having a marginal relationship with cyber victimization. Another theoretical predictor, association with deviant cyber peers, was a significant predictor across all models. While the victim-offender overlap for traditional offenses and cyber deviance (i.e cyber bullying) are plentiful, studies of the cybercrime victim-offender overlap remain limited. As this is one of only a handful of empirical examinations of this relationship, further study of theoretical predictors in this overlap are needed.

References

Akers, R. L. (1973). *Deviant behavior: A social learning approach.* Wadsworth Publishing Company.

Bachmann, M. (2010). The Risk Propensity and Rationality of Computer Hackers. *International Journal of Cyber Criminology* 4:643-656.

Berg, M.T., & Felson, R.B. (2016). Why are offenders victimized so often? *The Wiley handbook on the psychology of violence*, 49-65.

Berg, M.T., Stewart, E.A., Schreck, C.J., & Simons, R.L. (2012). The Victim–Offender Overlap in Context: Examining the Role of Neighborhood Street Culture. *Criminology 50*(2), 359–90. doi:10.1111/j.17459125.2011.00265.x.

Boillot Fansher, A.K. (2017). *Risky dating behaviors in the technological age: Consideration of a new pathway to victimization* (Doctoral dissertation).

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),400-420.

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.

Bossler, A.M., Holt, T.J., & May, D.C. (2012). Predicting online harassment victimization among a juvenile population. *Youth & Society*, *44*(4), 500-523.

Choi, K. (2008). Computer crime victimization and integrated theory: An empirical assessment. *International Journal of Cyber Criminology*, *2*(1), 308-333.

Cooper, J. & Harrison, D.M. (2001). The social organization of audio piracy on the Internet. *Media*, *Culture & Society* 23:71-89.

Craig, W., Harel-Fisch, Y., Fogel-Grinvald, H., Dostaler, S., Hetland, J., Simons-Morton, B., Molcho, M., de Mato, M.G., Overpeck, M., Due, P. & Pickett, W. (2009). A Cross-National Profile of Bullying and Victimization among Adolescents in 40 Countries. *Journal of Public Health 54*(Suppl.2), 216–224.

Donner, Christopher M. (2016). The gender gap and cybercrime: an examination of college students' online offending. *Victims & Offenders*, *11*(4), 556-577.

Donner, C.M., Marcum, C.D., Jennings, W.G., Higgins, G.E., & Banfield, J. (2014). Low self-control and cybercrime: Exploring the utility of the general theory of crime beyond digital piracy. *Computers in Human Behavior*, *34*, 165-172.

Eining, M.M., & Christensen, A.L. (1991). A Psycho-Social Model of Software Piracy: The Development and Test of a Model. In R.M. Dejoie, G.C. Fowler, and D.B. Paradice (Eds.), *Ethical Issues in Information Systems* (pp. 182-188). Boston, MA: Boyd and Fraser.

Evans, T.D., Cullen, F.T., Burton, Jr., V.S., Dunaway, R.G., & Benson, M.L. (1997). The Social Consequences of Self-control: Testing the General Theory of Crime. *Criminology 35*, 475-501.

Facts + Statistics: Identity theft and cybercrime. n.d.. In *Insurance Inforamtion Institute*. Retrieved from

Forde, D.R., & Kennedy, L.W. (1997). Risky lifestyles, routine activities, and the general theory of crime. *Justice Quarterly*, *14*(2), 265-294.

Foster, D.R. (2004). Can the general theory of crime account for computer offenders: Testing low self-control as a predictor of computer crime offending. Unpublished master thesis, University of Maryland, College Park.

Gibson, C., & Wright, J. (2001). Low Self-Control and Coworker Delinquency: A Research Note. *Journal of Criminal Justice 29(6)*, 483-492.

Gottfredson, M.R., & Hirschi, T. (1990). *A general theory of crime*. Stanford, Calif: 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.

Hay, C., & Evans, M.M. (2006). Violent Victimization and Involvement in Delinquency: Examining Predictions from General Strain Theory. *Journal of Criminal Justice 34*(3), 261–74. *doi:10.1016/j.jcrimjus.2006.03.005.*

Higgins, G.E. (2007). Digital piracy, self-control theory, and rational choice: An examination of the role of value. *International Journal of Cyber Criminology*, *1*(1), 33-55.

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). Self-control, deviant peers, and software piracy. *Psychological reports*, *95*(3), 921-931.

Higgins, G.E., Tewksbury, R., & Mustaine, E.E. (2007). Sports fan binge drinking: An examination using low self-control and peer association. *Sociological Spectrum*, *27*(4), 389-404.

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. (2001). Correlates of Internet software piracy. *Journal of Contemporary Criminal Justice*, *17*(4), 369-382.

Hinduja, S. (2003). Trends and patterns among online software pirates. *Ethics and Information Technology*, *5*(1), 49-61.

Hinduja, S., & Ingram, J.R. (2008). Self-Control and Ethical Beliefs on the Social Learning of Intellectual Property Theft. *Western Criminological Review 9(*2), 52-72.

Hinduja, S., & Ingram, J.R. (2009). Social learning theory and music piracy: The differential role of online and offline peer influences. *Criminal Justice Studies*, *22*(4), 405-420.

Hinduja, S., & Patchin, J.W. (2008). Cyberbullying: An exploratory analysis of factors related to offending and victimization. *Deviant behavior*, *29*(2), 129-156.

Hinduja, S., & Patchin, J.W. (2009). Bullying beyond the Schoolyard: Preventing and Responding to Cyberbullying. Thousand Oaks, CA: Sage Publication.

Hollinger, R.C. (1993). Crime by Computer: Correlates of Software Piracy and Unauthorized Account Access. *Security Journal 4(1)*, 2-12.

Holt, T.J., & Bossler, A.M. (2013). Examining the relationship between routine activities and malware infection indicators. *Journal of Contemporary Criminal Justice*, *29*(4), 420-436.

Holt, T.J., & Bossler, A.M. (2014). An assessment of the current state of cybercrime scholarship. *Deviant Behavior*, *35*(1), 20-40.

Holt, T.J., Bossler, A.M., Malinski, R., & May, D.C. (2016). Identifying predictors of unwanted online sexual conversations among youth using a low self-control and routine activity framework. *Journal of Contemporary Criminal Justice*, *32*(2), 108-128.

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., Burruss, G.W., & Bossler, A.M. (2010). Social learning and cyber-deviance: Examining the importance of a full social learning model in the virtual world. *Journal of Crime and Justice*, *33*(2), 31-61.

Holt, T.J., & Copes, H. (2010). Transferring subcultural knowledge on-line: Practices and beliefs of persistent digital pirates. *Deviant Behavior*, *31*(7), 625-654.

Holt, T.J., & Turner, M.G. (2012). Examining Risks and Protective Factors of On Line Identity Theft. Deviant Behavior 33(4), *308–323.*

Holtfreter, K., Reisig, M.D., & Pratt, T.C. (2008). Low self-control, routine activities, and fraud victimization. *Criminology*, *46*(1), 189-220.

Jennings, W.G., Piquero, A.R., & Reingle, J.M. (2012). On the overlap between victimization and offending: A review of the literature. *Aggression and Violent behavior*, *17*(1), 16-26.

Joinson, A. (1998). Causes and Implications of Behavior on the Internet. Pp. 43–60 in *Psychology and the Internet: Intrapersonal, Interpersonal, and Transpersonal Implications*, edited by J. Gackenbach. San Diego, CA: Academic Press.

Jordan, T. & Taylor, P. (1998). A sociology of hackers. *The Sociological Review*, 46(4): 757-780.

Kerstens, J., & Jansen, J. (2016). The victim–perpetrator overlap in financial cybercrime: Evidence and reflection on the overlap of youth's on-line victimization and perpetration. *Deviant Behavior*, *37*(5), 585-600.

Lauritsen, J.L., & Laub, J.H. (2007). Understanding the Link between Victimization and Offending: New Reflections on an Old Idea. *Crime Prevention Studies 22*, 55–75.

Lauritsen, J.L., Sampson, R.J., & Laub, J.H. (1991). The Link between Offending and Victimization among Adolescents. *Criminology 29*(2):265–92. doi:10.1111/j.1745-9125.1991.tb01067.x.

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.

Malin, J., & Fowers, B.J. (2009). Adolescent self-control and music and movie piracy. *Computers in Human Behavior 25(3)*, 718-722.

Marcum, C.D., Higgins, G.E., & Ricketts, M.L. (2014a). Juveniles and Cyber Stalking in the United States: An Analysis of Theoretical Predictors of Patterns of Online Perpetration. *International Journal of Cyber Criminology*, *8*(1). 47-56.

Marcum, C.D., Higgins, G.E., & Ricketts, M.L. (2014b). Sexting behaviors among adolescents in rural North Carolina: a theoretical examination of low self-control and deviant peer association. *International Journal of Cyber Criminology*, *8*(2), 68-79.

Miller, B., & Morris, R.G. (2016). Virtual peer effects in social learning theory. *Crime & Delinquency*, *62*(12), 1543-1569.

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.

Morris, R.G., & Higgins, G.E. (2009) Neutralizing Potential and Self-Reported Digital Piracy: A Multitheoretical Exploration Among College Undergraduates. *Criminal Justice Review 34*(2), 173-195.

Morris, R.G., & Higgins, G.E. (2010). Criminological Theory in the Digital Age: The Case of Social Learning Theory and Digital Piracy. *Journal of Criminal Justice 38*(4), 470-480.

Nodeland, B., & Morris, R.G. (2020a). A Test of Social Learning Theory and Self-Control on Cyber Offending. *Deviant Behavior*,*41*(1), 41-56.

Nodeland, B., & Morris, R. (2020b). The Impact of Low Self-control on Past and Future Cyber Offending. *International Journal of Cyber Criminology*, *14*(1), 106-120.

Ngo, F.T., & Paternoster, R. (2011). Cybercrime Victimization: An examination of Individual and Situational level factors. *International Journal of Cyber Criminology*, *5*(1).

Pratt, T.C., Turanovic, J.J., Fox, K.A., & Wright, K.A. (2014). Self-control and victimization: A meta-analysis. *Criminology, 52*(1), 87-116.

Ousey, G.C., Wilcox, P., & Fisher, B.S. (2011). Something Old, Something New: Revisiting Competing Hypotheses of the Victimization-Offending Relationship among Adolescents. *Journal of Quantitative Criminology 27*(1):53–84. doi:10.1007/s10940-010-9099-1.

Piquero, A.R., MacDonald, J., Dobrin, A., Daigle, L.E., & Cullen, F.T. (2005). Self-Control, Violent Offending, and Homicide Victimization: Assessing the General Theory of Crime. *Journal of Quantitative Criminology 21*(1), 55-71.

Pratt, T., & Cullen, F. (2000). The Empirical Status of Gottfredson and Hirschi's General Theory of Crime: A Meta-Analysis. *Criminology 38*(3), 931-964.

Pratt, T.C., Holtfreter, K., & Reisig, M.D. (2010). Routine On-line Activity and Internet Fraud Targeting: Extending the Generality of Routine Activity Theory. *Journal of Research in Crime and Delinquency 47(3), 267–296.*

Pratt, T. C., Turanovic, J. J., Fox, K. A., & Wright, K. A. (2014). Self-control and victimization: A meta-analysis. *Criminology*, *52*(1), 87-116.

Reyns, B.W. (2019). Online pursuit in the twilight zone: cyberstalking perpetration by college students. *Victims & Offenders*, *14*(2), 183-198.

Reyns, B.W., Burek, M.W., Henson, B., & Fisher, B.S. (2013). The unintended consequences of digital technology: Exploring the relationship between sexting and cybervictimization. *Journal of Crime and Justice*, *36*(1), 1-17.

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. *International journal of offender therapy and comparative criminology*, *60*(10), 1119-1139.

Reyns, B.W., Fisher, B.S., Bossler, A.M., & Holt, T. J. (2019). Opportunity and Self-Control: Do they Predict Multiple Forms of Online Victimization?. *American Journal of Criminal Justice*, *44*(1), 63-82.

Schreck, C.J. (1999). Criminal victimization and low self-control: An extension and test of a general theory of crime. *Justice Quarterly, 16*(3), 633-654.

Schreck, C.J., Fisher, B.S., & Miller, J.M. (2003). The social context of violent victimization: A study of the delinquent peer effect. *Justice Quarterly*, *21*(1), 23-47.

Schreck, C.J., Stewart, E.A., & Fisher, B.S. (2006). Self-control, victimization, and their influence on risky lifestyles: A longitudinal analysis using panel data. *Journal of Quantitative Criminology*, *22*(4), 319-340.

Schreck, C.J., Stewart, E.A., & Osgood, D.W. (2008). A Reappraisal of the Overlap of Violent Offenders and Victims. *Criminology 46*(4), 871–906. doi:10.1111/j.1745-9125.2008.00127.x.

Schreck, C.J., Wright, R.A., & Miller, J.M. (2002). A study of individual and situational antecedents of violent victimization. *Justice Quarterly*, *19*(1), 159-180.

Seale, D.A., Polakowski, M. & Schneider, S. (1998). It's not really theft!: personal and workplace ethics that enable software piracy. *Behaviour & Information Technology*, *17*(1), 27-40.

Sims, R.R., Cheng, H.K., & Teegen, H. (1996). Toward a Profile of Student Software Pirates, *Journal of Business Ethics*, *15,* 839-849.

Skinner, W.F. & Fream, A.M. (1997). A Social Learning Theory Analysis of Computer Crime Among College Student. *Journal of Research in Crime and Delinquency*, 34(4): 495-518.

Slonje, R., & Smith, P.K. (2008). Cyberbullying: Another Main Type of Bullying. *Scandinavian Journal of Psychology* 49(2), 147–154. doi:10.1111/j.1467-9450.2007.00611.x

Solomon, S.L., & O'Brien, J.A. (1990). The Effect of Demographic Factors on Attitudes toward Software Piracy, *Journal of Information Systems*, 30(3), 40-46.

Stewart, E.A., Elifson, K.W., & Sterk, C.E. (2004). Integrating the general theory of crime into an explanation of violent victimization among female offenders. *Justice Quarterly*, *21*(1), 159-181.

Suler, J. (2004). The Online Disinhibition Effect. *Cyber Psychology & Behavior* 7(3), 321–326. doi:10.1089/ 1094931041291295

Tangney, J. P., Baumeister, R. F., & Boone, A. L. (2004). High self-control predicts good adjustment, less pathology, better grades, and interpersonal success. *Journal of personality*, 72(2), 271-324.

Van Gelder, J.L., Averdijk, M., Eisner, M., & Ribaud, D. (2015). Unpacking the victim-offender overlap: On role differentiation and socio-psychological characteristics. *Journal of Quantitative Criminology*, *31*(4), 653-675.

Vandebosch, H., & van Cleemput, K. (2009). Cyberbullying among Youngsters: Profiles of Bullies and Victims. *New Media & Society* 11(8), 1349–1371.

Vazsonyi, A. T., Mikuška, J., & Kelley, E. L. (2017). It's time: A meta-analysis on the self-control-deviance link. *Journal of Criminal Justice*, *48*, 48-63.

Wall, D. (2007). Cybercrime: The Transformation of Crime in the Information Age. Cambridge, UK: Polity Press.

Warr, M. (2002). Companions in crime: The social aspects of criminal conduct. New York: Cambridge University Press.

Weulen Kranenbarg, M., Holt, T. J., & van Gelder, J. L. (2019). Offending and victimization in the digital age: Comparing correlates of cybercrime and traditional offending-only, victimization-only and the victimization-offending overlap. *Deviant Behavior*, *40*(1), 40-55.

Wolfe, S.E., Higgins, G.E., & Marcum, C.D. (2008). Deterrence and digital piracy: A preliminary examination of the role of viruses. *Social Science Computer Review*, *26*(3), 317-333.

Ybarra, M.L., & Mitchell, K.J. (2004). Online Aggressor/Targets, Aggressors, and Targets: A Comparison of Associated Youth Characteristics. *Journal of Child Psychology and Psychiatry 45*(7),

1308–1316.