Deviant Behavior

ISSN: 0163-9625 (Print) 1521-0456 (Online) Journal homepage: http://www.tandfonline.com/loi/udbh20

Offending and Victimization in the Digital Age: Comparing Correlates of Cybercrime and Traditional Offending-Only, Victimization-Only and the Victimization-Offending Overlap

Marleen Weulen Kranenbarg, Thomas J. Holt & Jean-Louis van Gelder

To cite this article: Marleen Weulen Kranenbarg, Thomas J. Holt & Jean-Louis van Gelder (2017): Offending and Victimization in the Digital Age: Comparing Correlates of Cybercrime and Traditional Offending-Only, Victimization-Only and the Victimization-Offending Overlap, Deviant Behavior, DOI: 10.1080/01639625.2017.1411030

To link to this article: https://doi.org/10.1080/01639625.2017.1411030

Published online: 11 Dec 2017.

DEVIANT BEHAVIOR
https://doi.org/10.1080/01639625.2017.1411030

Routledge
Taylor & Francis Group

Offending and Victimization in the Digital Age: Comparing Correlates of Cybercrime and Traditional Offending-Only, Victimization-Only and the Victimization-Offending Overlap

Marleen Weulen Kranenbarg [a], Thomas J. Holt[b], and Jean-Louis van Gelder[c]

[a]Department of Criminology, Faculty of Law, Vrije Universiteit Amsterdam, The Netherlands; [b]School of Criminal Justice, Michigan State University, East Lansing, Michigan, USA; [c]Netherlands Institute for the Study of Crime and Law Enforcement (NSCR), Amsterdam, The Netherlands

ABSTRACT

Cybercrime research suggests that, analogous to traditional crime, victims are more likely to be offenders. This overlap could be caused by shared risk factors, but it is unclear if these are comparable to traditional risk factors. Utilizing a high risk sample of computer-dependent cyber-offenders and traditional offenders (N = 535) we compare victimization, offending, and victimization-offending between cybercrime and traditional crime. Cybercrime results show a considerable victim-offender overlap and correlates like low self-control and routine activities partly explain differences in victimization, offending, and victimization-offending. Some cybercrime correlates are related to the digital context, but show similar patterns for cybercrime and traditional crime.

ARTICLE HISTORY
Received 24 May 2017
Accepted 23 August 2017

Introduction

Recent research demonstrates that there has been a significant rise in the rate of crimes that utilize information technology (IT) systems over the last two decades, though the rate of traditional crimes has decreased. Crime statistics in the United Kingdom now show that 'crime has not actually fallen but changed, moving to newer forms of crime' (Office for National Statistics 2015). Tcherni and colleagues (2016) found that online property crime rates show a wave in crime that 'may override any benefits Americans have enjoyed as a result of the steady drop in traditional forms of property crime' (906). These new crimes take place in a digital context where, unlike many traditional forms of crime, there is no physical convergence in space and time of offenders and victims (e.g., Bossler and Holt 2009; Holt and Bossler 2008; Kerstens and Jansen 2016; Suler 2004; Yar 2005). This raises the question as to whether traditional correlates of offending and victimization can account for cybercrime offending and victimization.

For traditional crimes, a large body of research has shown that victims are likely to commit criminal acts, and that offenders have a relatively high probability of being victimized (e.g., Berg et al. 2012; Averdijk et al. 2016; Hay and Evans 2006; Lauritsen and Laub 2007; Lauritsen, Sampson, and Laub 1991; Ousey, Wilcox, and Fisher 2011; Schreck, Stewart and Osgood 2008). This research has *inter alia* shown that victims and offenders share risk factors like low self-control, routine activities or a risky life-style and socio-demographics that increase both their risk for offending and victimization. In addition, offending can directly cause victimization or vice versa (for a review see Berg and Felson 2016; Jennings, Piquero, and Reingle 2012; Lauritsen and Laub 2007). It should be noted that only a part of the offender population is at risk of victimization, and not all victims commit crimes. Therefore scholars recently stressed the importance of studying victims-only,

CONTACT Marleen Weulen Kranenbarg M.WeulenKranenbarg@vu.nl De Boelelaan 1105, 1081 HV Amsterdam, The Netherlands

offenders-only, and victim-offenders as separate groups to clearly identify any differences in underlying risk factors (e.g., Schreck, Stewart, and Wayne Osgood 2008; Van Gelder et al. 2015).

Although cybercrime offending and victimization have largely been studied separately, there is evidence of shared risk factors, like low self-control and risky online routine activities (for a review see Holt and Bossler 2014). In fact, cybercrime offending has been found to be a risk factor for victimization and vice versa (e.g., Bossler and Holt 2009; Morris 2011; Ngo and Paternoster 2011; Wolfe, Higgins, and Marcum 2008). This indicates that cybercrime offending and victimization share similar underlying correlates, and as such should be studied in tandem, as is evident in traditional crimes.

For cybercrime, one study to date has specifically explored the possibility of a victim-offender overlap among youth (Kerstens and Jansen 2016). This study found a considerable crossover in financial cybercrime offending and victimization which was associated with low self-control, retaliation, high online disinhibition, and online routine activities (Kerstens and Jansen 2016). Since this study focused solely on financial cybercrime among youth, it is unclear if the overlap is evident in adult samples and in other types of cybercrime. In addition, previous research does not empirically compare cybercrime with traditional crime, limiting our understanding of any similarity in the correlates of these crime types.

The current study attempts to address these gaps in the literature by using an adult high risk population of former suspects from the Netherlands to assess their rates of cybercrime and traditional offending and victimization. The risk factors for offending and victimization are compared within offending-only, victimization-only and victimization-offending groups, for technical computer-dependent cybercrime (like hacking, data theft, defacing, etcetera) and traditional crime. Risk factors include low self-control, online and offline routine activities, and IT-skills. The results will show to what extent these risk factors can explain cybercrime offending and victimization in a way similar to traditional crime.

Risk factors for traditional crime and cybercrime

Situational and personal risk factors such as low self-control, risky life-styles or routine activities, substance abuse and socio-economic status are associated with both offending and victimization risks for traditional crimes (e.g., Berg and Felson 2016; Jennings, Piquero, and Reingle 2012). People, who spend more time with delinquent friends and/or in places where crimes take place, are more at risk of being victimized and also have more criminal opportunities (e.g., Jensen and Brownfield 1986; Lauritsen, Sampson, and Laub 1991; Sampson and Lauritsen 1990; Schreck, Wright and Miller 2002). In addition, impulsivity and low self-control can directly increase victimization and offending (e.g., Gottfredson and Hirschi 1990; Jennings et al. 2010; Piquero et al. 2005; Pratt et al. 2014), but also indirectly through the association between low self-control and increased time spent in criminogenic settings (e.g., Schreck 1999; Schreck, Stewart, and Fisher 2006). Similarly, substance abuse is a clear risk factor for traditional victimization and offending (e.g., Berg and Felson 2016; Longshore et al. 2004; Turanovic and Pratt 2013).

Cybercrimes tend to be committed in a different context than traditional crimes, which may lead to different risk factors for both offending and victimization. The relationship between traditional offending and victimization is the strongest for violent crimes, which as per definition requires physical interaction between victims and offenders (Berg and Felson 2016; Lauritsen and Laub 2007). In the case of cybercrime there is no physical convergence in space and time of offenders and victims (e.g., Bossler and Holt 2009; Holt and Bossler 2008; Yar 2005). Nevertheless, previous research suggests that victims and offenders eventually interact with one another in order for cybercrime to occur, even if it occurs asynchronously. This may account for the association identified between cybercrime offending and the increased risk of victimization, as well as common risk factors for both experiences, including low self-control, routine activities, and socio-demographic characteristics

(e.g., Bossler and Holt 2009; Holt and Bossler 2014; Ngo and Paternoster 2011; Wolfe, Higgins, and Marcum 2008).

Research examining the association between cybercrime offending and victimization has largely focused on forms of cybercrime that do not require technical expertise or are dependent on technology, such as fraud (Ngo and Paternoster 2011), bullying (Holt and Bossler 2008), or piracy (Wolfe, Higgins, and Marcum 2008). New and more technical computer-dependent crimes, like cyber-trespass (Wall 2001), have received less attention from researchers. For instance, research on malware victimization found individuals with malicious software infections were more likely to engage in online deviance, mainly piracy or viewing pornography (e.g., Bossler and Holt 2009; Choi 2008; Wolfe, Higgins, and Marcum 2008). When comparing online harassment with hacking victimization, Van Wilsem (2013) found that online offending was related to harassment but not to hacking.

Assessing the theoretical explanations for the victim-offender overlap

Considering the common risk factors associated with cybercrime victimization and offending, it is imperative to understand their underlying theoretical relationships. The primary risk factor identified across multiple studies of cybercrime is low self-control, though it has greater explanatory power for less-technical forms of cybercrime (Holt and Bossler 2014). Some forms of cybercrime are simple to complete, provide immediate gratification for the individual, and present multiple opportunities for offending, such as digital piracy (Holt and Bossler 2014). These same conditions may increase an individual's risk of victimization as savvy offenders may target those who are online more frequently and engage in risky activities like downloading pirated materials (Bossler and Holt 2010). Van Wilsem (2013) found that low self-control was positively related to hacking victimization, while Bossler and Holt (2010) found that low self-control was neither related to hacking nor to malware victimization. However, Holtfreter, Reisig, and Pratt (2008) found that although targeting is random, the personal characteristics and behavior of the victim influenced who responded to a scam. As a result, low self-control may play a role in the risk of victimization regardless of the targeted nature of victimization.

With respect to offending, it has been argued that advanced types of hacking and other technical computer-dependent cybercrimes require more self-control. Offenders must learn the skills needed in order to commit the act, such as manipulation of computer hardware and software via malicious software (Bossler and Burruss 2011). They must also have the patience to plan and execute the offense properly and cover their tracks (e.g., Holt and Kilger 2008). In contrast, some research has found that offenders who learn from friends do not need high self-control to be able to commit these crimes (Bossler and Burruss 2011; Holt, Bossler, and May 2012a). As the current study focuses on these computer-dependent cybercrimes, low self-control may be less important for cybercrime offending and victimization compared to traditional crime.

Routine activities theory

As a second risk factor, online routine activities enable the digital convergence of offenders and victims and may be associated with a cybercrime victim-offender overlap. Individual involvement in routine activities that increase exposure to motivated offenders may disproportionately increase the risk of victimization. To that end, several studies have found time spent in specific activities, like time spent using e-mail or social media, increases individual risks of interpersonal victimization such as online harassment (Bossler and Holt 2009; Holt and Bossler 2008; Leukfeldt 2014). In a recent study, based on a large representative sample, online communication, or use of forums or social networks increased hacking victimization (Leukfeldt and Yar 2016). Time spent using the internet, targeted and untargeted browsing, online shopping, downloading and gaming were all related to malware victimization (Leukfeldt and Yar 2016).

Studies that relate offending to life-style or routine activity measures are virtually non-existent for serious forms of cybercrime, such as complex hacks and the use of malicious software. Nevertheless,

studies have shown that spending time on social networks or online forums can provide offenders with the knowledge or social contacts to commit cybercrime (e.g., Holt et al. 2012b; Hutchings 2014). In addition, online gaming environments can increase opportunities and motivation for hacking, but could consequently also increase the risk for victimization. An example is hacking into gaming accounts to steal virtual objects or credits (Blackburn et al. 2014; Hu, Xu and Yayla 2013). Kerstens and Jansen (2016) also found that spending more time online results in a higher likelihood of being a victim-offender. This suggests that although there is no physical convergence of offenders and victims, the digital convergence of actors in online spaces can increase the risk of cybercrime victimization.

Studies of cybercrime victimization include online routine activities only, while studies of traditional crime only include offline daily routine activities like work or school, and nightlife activities like going out and being with friends (Lauritsen, Sampson, and Laub 1991). The absence of measures may lead to model misspecification as online activity could increase the risk of offline crimes like fraud (Holtfreter, Reisig, and Pratt 2008). At the same time, traditional crimes might decrease because individuals spend more time online (Tcherni et al. 2016). Consequently, both online and offline activities must be included in any analyses of cybercrime and traditional crime to more accurately assess the influence of behaviors on the risk of offending and victimization (Leukfeldt and Yar 2016).

In addition to the opportunities and risks created by routine activities, a person's technological skill could influence their opportunities for cybercrime offending as well as victimization risks. Individuals with greater technical expertise, acquired through social relationships and personal experience, may directly and indirectly increase a person's ability to engage in cyber-dependent crimes (Bossler and Burruss 2011; Chua and Holt 2016; Holt, Bossler, and May 2012a; Holt and Kilger 2008).

Technological capacity may also serve as a protective factor against cybercrime victimization, as it is thought technically proficient individuals can identify when their computer may have been compromised or utilize appropriate resources to secure their system. Most studies, however, find no relationship between IT-skills and malware infections (e.g., Bossler and Holt 2009; Ngo and Paternoster 2011), though some have found the opposite (e.g., Van Wilsem 2013). These contradictory findings may stem from differences in technology use as a function of IT-skills, which may increase the risk for victimization. Leukfeldt and Yar (2016) found that although computer knowledge in general was not related to hacking or malware victimization, operating system and browser type were related to malware victimization and risk awareness was negatively related to hacking victimization.

In addition, the link between socio-demographic factors that explain traditional offending and victimization and cybercrime is mixed. Previous research suggests that cybercrime offending, especially of more computer-dependent crimes, occurs in higher social classes (e.g., Pontell and Rosoff 2009) and victimization occurs more often among higher educated people (e.g., Leukfeldt and Yar 2016).

The current study

To address these issues, this analysis explores the correlates of offending and victimization for computer-dependent crimes like hacking, data theft, and defacing. We test whether the risk factors that have been found to predict cybercrime victimization and offending separately also explain victimization-offending, offending-only, and victimization-only. A comparative model is also developed for traditional offenses to compare the risk factors between cybercrime and 'real world' traditional crime.

Method

Sample and procedure

This study is based on a Dutch high risk sample of adult (18+) suspects of cybercrime and traditional crime. All 1,100 cybercrime suspects and a random sample of 1,127 traditional suspects from the period 2000–2013 were identified. Of this original sample, 172 cybercrime suspects (15.64%) and 252 traditional suspects (22.36%) either did not have a valid current mailing address, had a hidden

address or had passed away. The remaining 928 cybercrime suspects and 875 traditional suspects were invited by physical mail to participate in an online survey on computer and internet knowledge and their experiences with online and offline safety. In exchange for participation they would receive a €50 voucher. Respondents could participate by following the website link in the letter and entering their unique password. Respondents could request a paper version of the survey or complete the survey through a Tor Hidden Service website.[1] The former option was chosen by three traditional sample respondents, whereas three respondents of the cybercrime sample opted for the latter option.

The invitation letter also mentioned confidentiality and anonymity, which were further detailed on the first page of the survey. This page also included an online consent form, information about the selection procedure and more details about the purposes and content of the survey. Two weeks after sending the invitation 260 cybercrime suspects and 83 traditional suspects had completed the survey. A reminder was sent to the sample of traditional suspects. After a second reminder two weeks later 268 cybercrime suspects (28.88%) and 141 traditional suspects (16.11%) completed the full survey. As a third reminder would not have resulted in two equal samples of suspects, a new random sample of 781 traditional suspects was contacted using exactly the same procedure. After six weeks 126 of them (16.13%) completed the survey. The final sample consisted of 268 cybercrime suspects (28.88%) and 267 traditional suspects (16.12%), an average response rate of 20.70%.

For this analysis, 39 respondents (7.29%) were excluded because of missing values on one or more of the dependent variables, and 29 (5.42%) because of missing values on one of the independent variables. Validity checks on impossible response combinations or patterns resulted in the exclusion of another eight respondents (1.50%), resulting in a final sample of 459 respondents, 240 cybercrime suspects and 219 traditional suspects. For cybercrime suspects, females were overrepresented among respondents compared to non-respondents (20.00% compared to 13.37%, $X^2(1) = 6.10$, $p < 0.05$), and for traditional suspects respondents were relatively younger (*Myears* = 38.49 compared to *Myears* = 40.90, $t(1654) = 2.47$, $p < .05$).

Measures

Dependent variables

Victimization and offending in the preceding 12 months were measured using self-report questions with the following response categories: 0 times, 1 time, 2 times, 3–5 times, 6–10 times, more often. Victimization questions were introduced as follows: 'The following questions are about your experiences with online (digital) [traditional crime: offline (non-digital)] crime in the preceding twelve months. How often in the preceding twelve months…' followed by descriptions of different types of victimization. For example, malware victimization was measured by asking: 'How often in the preceding twelve months…' '… did malware (malicious software) damage your computer and/or the files on your computer?' And offline vandalism was measured by using the description: '… did somebody break or damage something that belonged to you, without stealing something?'. The survey included six types of cybercrime victimization: malware, hacking, phishing, defacing, data theft or damage, and DoS attacks. These items were formulated by using the overview of cybercrime types of the Dutch National Cyber Security Centre (2012). Eight types of traditional victimization, based on the Dutch Safety Monitor (Statistics Netherlands 2014), were included: bicycle theft, vandalism, other theft, threats, violence, attempted burglary, burglary, and sexual assault.

Offending questions for cybercrime were based on the description of computer-dependent cybercrimes of the Dutch National Cyber Security Centre (2012) and the Computer Crime Index developed by Rogers (2001). The items were introduced as:

> Many people sometimes do things that are not allowed or that are against the law. The following questions regard online (digital) activities you might have undertaken. Please answer as honestly as possible. In the preceding twelve months, how often did you, without permission …'

[1]Communication with this type of website is completely encrypted and less easy to trace.

followed by descriptions of different types of offending. For example: '… break in or log on to a network, computer or web account by guessing the password?' and: '… gain access to a network, computer, web account or files that were saved on it in another way?'. Thirteen types of cyber-offending were included: defacing, guessing passwords, digital theft, other types of hacking, damaging data, taking control over an IT-system, phishing, malware use, intercepting communication, DoS attacks, selling somebody else's data, spamming, and selling somebody else's credentials. Traditional crimes were introduced as:

> There are also offline things that are not allowed or are against the law, but many people sometimes do. The following questions regard offline (non-digital) activities you might have undertaken. Please answer as honestly as possible. In the preceding twelve months, how often …

followed by descriptions of offending types. For example, stealing: '… did you steal something worth more than five euros (from a person, on the street, from a house, from a store, at work, etc.)?'. Eleven types of traditional offending were included: tax fraud, stealing, threats, violence, buying or selling stolen goods, carrying a weapon, vandalism, selling drugs, insurance fraud, burglary, and using a weapon. These items were based on the self-report measure of Svensson et al. (2013) and Dutch criminal law.

All respondents who reported that they experienced at least one form of crime in the preceding twelve months were considered to be victims. All respondents who reported to have committed at least one crime were considered to be offenders. If both offending and victimization was reported, respondents were considered to be victim-offenders.

Independent variables

Low self-control. Low self-control was measured with items from the HEXACO-SPI-96 personality inventory (De Vries and Born 2013), which is especially suitable for lower educational levels and ethnic minorities with language difficulties. We followed the procedure used by Van Gelder and De Vries (2012) to construct a scale measure based on the self-control scale developed by Grasmick et al. (1993). To construct HEXACO Self-Control, Van Gelder and De Vries (2012) first selected those HEXACO facets that correlated most strongly with the Grasmick et al. self-control scale in a community sample representative of the Dutch adult population. Subsequently, they ran regressions using these facets with Grasmick et al. self-control as the dependent variable. Following this procedure, they arrived at the HEXACO Self-Control measure which is based on the regression weights expressed in the following formula: HEXACO Self-Control = (3*Prudence + 2*(Fairness + Modesty + Fearfulness + Flexibility) + (Social Self-esteem + Patience + Inquisitiveness + Diligence + Altruism))/16. We used a slightly modified version of the original HEXACO Self-Control scale version, with 15 instead of 16 items, as the original Altruism item was not included in the HEXACO-SPI-96. Altruism was therefore not included in our self-control scale. Self-control was reverse coded to a continuous low self-control measure. Descriptive statistics of all independent variables can be found in Table 1.

Online routine activities and IT-skills. Five online routine activities based on the online routines questionnaire of Domenie et al. (2013) were used: 1. online communication: 'e-mailing, chatting online or using social media (like Facebook, Twitter etc.)'; 2. 'online shopping'; 3. 'gaming'; 4. forum use: 'reading Internet forums and/or posting messages on these forums'; and 5. 'programming'. These items capture both general and common online activities and more specific as well as less common types of activities. Respondents indicated how many hours per week they spend on those activities, during leisure time and work during an average week: 0 = 0 hours, 1 = 1–5 hours, 2 = 6–10 hours, 3 = 11–20 hours, 4 = 21 hours or more.

IT-skills were measured using a translated version of the IT-skills measure developed by Holt, Bossler, and May (2012a), which is based on Rogers (2001). We added an extra statement to capture the high skill level that some of the respondents were expected to have. Respondents were asked to

Table 1. Descriptive statistics independent variables (N = 459).

	M	SD		*M*	SD
Online routines			Offline routines		
Communication	2.05	1.18	At work	2.81	1.61
Shopping	0.71	0.69	At school	0.44	1.11
Gaming	0.83	1.18	At home of friends	1.08	0.71
Forum use	0.74	0.92	Other with friends	1.18	0.89
Programming	0.46	1.07	Going out	0.87	0.70
IT-skills	1.92	1.04	Alcohol abuse	0.25	0.57
			Marijuana use	0.38	0.97
Low self-control	1.73	0.43	Dummy variables	*N*	%
Background characteristics			Male	358	78.00
Age	37.04	13.39	Living with family	246	53.59
Financial situation	0.24	0.27	Living with parents	80	17.43

M = Mean
SD = Standard Deviation

indicate which of these statements were most applicable: 0. 'I don't like using computers and don't use them unless I absolutely have to' 1. 'I can surf the net, use some common software but not fix my own computer' 2. 'I can use a variety of software and fix some computer problems I have' 3. 'I can use Linux, most software, and fix most computer problems I have' 4. 'I can use different programming languages and am capable of detecting programming errors'. This resulted in a continuous measure of IT-skills ranging from 0–4. This measure seemed to capture IT-skills well, and showed high convergent validity when comparing it to an objective IT-skills test that was also included in this survey (Pearson's r = .74, p < .001).

Offline routines and substance abuse. Offline routines were measured in the same way as online routines. In line with previous research, we included both daily activities and other outside the own home activities, based on items of the TransAm study (Blokland 2014). The activities we included were: 1. 'being at work'; 2. 'being at school'; 3. 'being at the home of my friends'; 4. 'being somewhere else with friends'; 5. 'going out (e.g., pub, club, restaurant, movies, etc.)'. In addition we asked respondents about their substance abuse, using items from Bernasco et al. (2013). We asked them to indicate: 1. 'How often does it happen that you cannot control yourself because you drank too much alcohol?' and 2. 'How often do you smoke weed or hashish?'. Response options were: 0 = never, 1 = less than once a month, 2 = once or a few times a month, 3 = once or a few times a week, 4 = (almost) every day.

Demographics. We controlled for gender (1 = male), age, living situation, and financial situation. Two dummy variables for living situation were included: living with family (partner and/or child) and living with parents. Financial situation was based on a scale of the level of financial problems, an adjusted version of the one used in The Prison Project study (Dirkzwager and Nieuwbeerta (unpublished)). Respondents indicated if the following situations occurred in the preceding twelve months (1 = yes): 1. 'saved money' 2. 'had just enough money to live' 3. 'had problems with making ends meet' 4. 'not been able to replace broken stuff' 5. 'had to borrow money for necessary expenses' 6. 'pledged belongings' 7. 'had creditors/bailiffs coming to my door' 8. 'had debts of 5.000 euros or more'. After reverse coding item 1, the sum of all items was divided by eight to obtain a scale ranging from 0–1 (α = 0.82). In addition, to control for the initial differences between the groups of cybercrime and traditional suspects, a dummy variable indicating the initial group was included (1 = cybercrime suspect).

Results

For both cybercrime and traditional crime there appeared to be a considerable victim-offender overlap (cybercrime victim-offender 9.59%, offender-only 8.06%, victim-only 28.98%, traditional

victim-offender 13.73%, offender-only 6.75%, victim-only 30.50%). When comparing prevalence rates of victimization and offending between the groups (Tables 2 and **3**), both types of victim-offenders experienced significantly more types of victimization. For cybercrime, only malware victimization is more common among victims-only, all other types are more common among victim-offenders. For traditional crime, bicycle theft is the only crime more common among victims-only and threats and violence are significantly more common among victim-offenders. For offending there is no significant difference in the number of different crime types committed by offenders-only and victim-offenders. More technical cybercrimes appear more common among offenders-only. For instance, hacking by guessing a password is more often committed by victim-offenders (marginally significant: $X^2(1) = 3.01$, $p = .08$), while hacking in another way is more often committed by offenders-only. Among victim-offenders of traditional crime violence is more common (marginally significant: $X^2(1) = 3.18$, $p = .07$).

Table 2. Prevalence rates victimization.

Cybercrime victimization					Traditional victimization				
	Victim-only		Victim-offender			Victim-only		Victim-offender	
	N	%	*N*	%		*N*	%	*N*	%
Malware	102	76.69	30	68.18	Attempted burglary	20	14.29	10	15.87
Hacking	35	26.32	17	38.64	Burglary	8	5.71	8	12.70
Data theft/damage	12	9.02	11	25.00**	Bicycle theft	66	47.14	28	44.44
Defacing	15	11.28	9	20.45	Other theft	45	32.14	28	44.44
DoS	12	9.02	6	13.64	Vandalism	50	35.71	30	47.62
Phishing	26	19.55	10	22.73	Threats	35	25.00	29	46.03**
					Violence	16	11.43	20	31.75***
					Sexual assault	8	5.71	6	9.52
	M	SD	M	SD		M	SD	M	SD
Types of victimization	1.52	0.96	1.89	1.20*		1.77	1.24	2.52	1.67***

* $p < .05$; ** $p < .01$; *** $p < .001$
M = Mean
SD = Standard Deviation

Table 3. Prevalence rates offending.

Cybercrime offending					Traditional offending				
	Offender-only		Victim-offender			Offender-only		Victim-offender	
	N	%	*N*	%		*N*	%	*N*	%
Guessing password	9	24.32	16	36.36	Stealing	8	25.81	15	23.81
Hacking	13	35.14	8	18.18	Burglary	0	0.00	3	4.76
Selling credentials	0	0.00	1	2.27	Stolen goods	4	12.90	14	22.22
Damaging data	7	18.92	9	20.45	Tax fraud	14	45.16	18	28.57
Digital theft	12	32.43	12	27.27	Insurance fraud	3	9.68	9	14.29
Selling data	1	2.70	3	6.82	Vandalism	3	9.68	12	19.05
Malware	3	8.11	6	13.64	Threats	5	16.13	18	28.57
Taking control	8	21.62	7	15.91	Carry weapon	6	19.35	12	19.05
Defacing	12	32.43	14	31.82	Violence	3	9.68	16	25.40
Intercepting comm.	5	13.51	3	6.82	Using weapon	0	0.00	2	3.17
DoS	1	2.70	4	9.09	Selling drugs	4	12.90	10	15.87
Phishing	6	16.22	7	15.91					
Spam	1	2.70	3	6.82					
	M	SD	M	SD		M	SD	M	SD
Types of offending	2.11	1.54	2.11	1.67		1.61	0.95	2.05	1.60

M = Mean
SD = Standard Deviation

Multinomial analyses

This section will first discuss the results for cybercrime and traditional crime separately and then compare those results. Table 4 shows the results from the multinomial logit analyses for cybercrime and traditional crime and the comparison between them. For comparing estimates within and between the models we used the seemingly unrelated estimation procedure as developed for Stata (Weesie 1999), as this method allows for testing between models based on the same, different, or partially overlapping datasets.

Cybercrime

Low self-control is an important predictor for being a cybercrime victim-offender. This is significantly stronger compared to victims-only ($X^2(1) = 7.42$, $p < .01$) and offenders-only ($X^2(1) = 4.95$, $p < .05$). In addition, having more IT-skills and spending more time on online shopping also increases the likelihood of victimization-offending. The effect of online shopping is significantly stronger compared to offenders-only and victims-only ($X^2(1) = 3.88$, $p < .05$ and ($X^2(1) = 6.69$, $p < .05$). In addition, the effect of online communication is stronger for victim-offenders compared to offenders-only ($X^2(1) = 4.33$, $p < .05$). Living with parents and being in the initial group of cybercrime suspects is also positively related to cybercrime victimization-offending. The effect of living with parents is even in the opposite direction for offenders-only and that difference is significant ($X^2(1) = 5.81$, $p < .05$).

A person is more likely to be an offender-only if more time is spent on forums or if a person has more IT-skills. This effect of forum use differs significantly from the effect for victim-offenders and victims-only ($X^2(1) = 8.58$, $p < .01$ and $X^2(1) = 7.97$, $p < .01$, respectively). Those effects are in the opposite direction. More IT-skills also significantly increase the likelihood of victimization-offending, but it is stronger for offending-only. Victims-only spent significantly less time on programming and they are more likely living with a family than alone. The results show that victim-offenders have a more general risk profile, while offenders-only have more IT-skills and specific online routines, and victims-only have less IT-skills and less personal risk factors.

Traditional crime

Alcohol abuse is significantly related to both offending and victimization-offending, while going out is related to victimization-only but not to the other two. The effects of going out and alcohol abuse also differ significantly between offenders-only and victims-only ($X^2(1) = 6.11$, $p < .05$ and $X^2(1) = 4.61$, $p < .05$). For victim-offenders there is also a significant effect of low self-control and spending more time outside with friends. The effect of spending time outside with friends also differs significantly between victims-only and victim-offenders ($X^2(1) = 6.08$, $p < .05$). There are no significant differences between offenders-only and victim-offenders. In addition to alcohol abuse, online shopping is positively related to offending-only, while people who live with family are less likely to be offenders-only than people who live alone, just like people who spend more time programming.

Spending more time on going out increases victimization-only, while marijuana use, living with parents and age are negatively related to victimization-only. The effect of marijuana use is in the opposite direction for victim-offenders and that difference is significant ($X^2(1) = 9.27$, $p < .01$). Lastly, victim-offenders report more financial problems. The effects of alcohol abuse, online shopping, and programming differ significantly between offenders-only and victims-only ($X^2(1) = 4.61$, $p < .05$; $X^2(1) = 5.09$, $p < .05$; $X^2(1) = 9.31$, $p < .01$). Overall, victim-offenders have more personal and situational risk factors than offenders-only and victims-only, but offenders-only and victim-offenders are more similar than victims-only.

Comparison

Between model comparisons show that overall the effects in the models are significantly different between cybercrime and traditional crime, for offenders-only, victims-only and victim-offenders.

Table 4. Multinomial logit models and between model comparisons.

	Cybercrime[1]						Traditional crime[2]						Model comparisons[3]		
	Offender-only		Victim-only		Victim-Offender		Offender-only		Victim-only		Victim-offender		Offender-only	Victim-only	Victim-offender
	OR	SE	OR	SE	OR	SE	OR	SE	OR	SE	OR	SE	X^2(DF)	X^2(DF)	X^2(DF)
Low self-control	1.43	0.68	1.31	0.37	4.05	1.91**	1.93	0.99	1.35	0.38	2.64	1.01*	0.29(1)	0.01(1)	0.58(1)
Online routines													20.39(6)**	8.54(6)	14.61(6)*
Communication	0.74	0.14	1.21	0.13	1.17	0.20	1.01	0.19	0.92	0.10	0.88	0.13	1.51(1)	3.81(1)	2.06(1)
Shopping	0.82	0.28	0.82	0.16	1.75	0.46*	1.83	0.57*	0.99	0.19	1.31	0.33	3.80(1)	0.73(1)	0.64(1)
Gaming	1.06	0.18	1.15	0.13	1.22	0.20	1.27	0.22	1.07	0.12	1.16	0.17	0.40(1)	0.18(1)	0.06(1)
Forum use	1.60	0.35*	0.83	0.12	0.64	0.15	0.93	0.24	0.92	0.14	1.00	0.19	2.23(1)	0.25(1)	
Programming	0.97	0.18	0.67	0.11*	0.83	0.17	0.45	0.15*	1.01	0.13	0.71	0.16	5.93(1)*	4.01(1)*	0.26(1)
IT-skills	1.89	0.48*	1.23	0.19	1.66	0.41*	1.23	0.35	1.08	0.17	0.84	0.18	1.55(1)	0.41(1)	5.04(1)*
Offline routines													9.54(7)	12.49(7)	6.94(7)
At work	1.03	0.33	1.37	0.26	1.58	0.45	0.85	0.29	1.26	0.24	0.82	0.21	0.19(1)	0.09(1)	3.32(1)
At school	1.39	0.39	1.08	0.19	1.38	0.35	1.49	0.44	1.00	0.18	1.73	0.39	0.03(1)	0.10(1)	0.53(1)
At home of friends	1.26	0.19	1.04	0.08	1.06	0.14	1.23	0.19	1.00	0.08	1.13	0.12	0.01(1)	0.14(1)	0.12(1)
Other with friends	1.07	0.18	0.96	0.13	0.92	0.16	1.28	0.26	1.11	0.14	1.20	0.19*	0.52(1)	1.03(1)	1.75(1)
Going out	1.48	0.48	0.85	0.17	0.86	0.26	0.59	0.21	1.53	0.32*	1.01	0.27	3.67(1)	4.63(1)*	0.16(1)
Alcohol abuse	0.83	0.29	0.83	0.19	1.33	0.38	2.11	0.72*	1.09	0.27	1.79	0.49*	3.55(1)	0.64(1)	0.53(1)
Marijuana use	1.19	0.22	1.21	0.16	1.39	0.25	0.96	0.23	0.72	0.11*	1.25	0.19	0.52(1)	5.98(1)*	0.25(1)
Background characteristics													4.74(5)	17.57(5)**	11.02(5)
Male	0.34	0.19	1.07	0.31	0.88	0.44	1.36	0.86	0.60	0.18	0.82	0.34	2.91(1)	2.37(1)	0.01(1)
Age	0.99	0.02	1.01	0.01	0.99	0.02	0.99	0.02	0.98	0.01*	0.99	0.02	0.00(1)	4.92(1)*	0.03(1)
Living with family	0.44	0.21	1.91	0.57*	1.55	0.80	0.35	0.18*	0.74	0.22	0.51	0.20	0.12(1)	5.54(1)*	3.36(1)
Living with parents	0.60	0.35	1.74	0.69	3.26	1.72*	0.28	0.19	0.43	0.17*	0.59	0.28	0.64(1)	7.88(1)**	7.56(1)*
Financial situation	3.53	2.62	1.35	0.62	1.63	1.25	1.50	1.25	2.04	0.96	3.80	2.34*	0.64(1)	0.42(1)	0.76(1)
Initial group	1.83	0.85	1.29	0.32	2.41	1.03*	1.15	0.54	0.74	0.19	1.05	0.37	0.60(1)	2.94(1)	2.50(1)
Combined comparison													33.52(20)*	47.82(20)***	44.29(20)**
N		37		133		44		31		140		63			

* p < .05; ** p < .01; *** p < .001

1. LR $X^2(60) = 127.73$; Reference group is: neither victim nor offender cybercrime ($N = 245$)
2. LR $X^2(60) = 118.33$; Reference group is: neither victim nor offender traditional crime ($N = 225$)
3. This table only includes between model comparisons of cybercrime and traditional crime. Significant differences within the models, between offenders-only, victims-only and victim-offenders are discussed in the text. Those comparisons can be requested from the first author.

OR = Odds Ratio
SE = Standard Error
X^2 = Chi-squared
DF = Degrees of freedom

The combined effects of online routines are significantly different between offenders-only and victim-offenders, while the combined effects of the background characteristics are significantly different for victims-only. There is no difference in the effects of low self-control and the combined effects of offline routines. The likelihood ratio chi-square tests show that the variables included in these models are better able to explain the differences in cybercrime offending-only, victimization-only and victimization-offending than traditional crime (even when excluding the initial group variable, results not shown).

There are substantive differences in the victim-only models for traditional and cybercrime, particularly for programming, going out, drug use, age and both living situations. As the overall effects of online and offline routines do not differ significantly between both groups of victims-only, the differences in the living situations are important. For offenders-only the effect of programming differs significantly. Where programming significantly reduces traditional offending it cannot reduce cybercrime offending. As the overall effect of online routines is also significantly different, cybercrime offenders-only are very different from traditional offenders-only in their online behavior and IT-skills. For victim-offenders the effects of IT-skills and living with parents differ significantly. Living with parents is marginally significant for traditional offenders, (p = .085). Overall, the most striking difference can be found in online routine activities, IT-skills, and living situations.

Discussion

In this study we compared traditional crime with a new and fast growing type of crime, which takes place in a different context: cybercrime. We examined both situational and personal correlates of cybercrime offending-only, victimization-only and victimization-offending separately. In addition, the empirical comparison with traditional crimes enabled us to examine the extent to which risk factors like risky routine activities and low self-control underlie this type of crime. By using an adult, high risk sample of former suspects, we were able to study computer-dependent cybercrime and make a meaningful comparison with traditional crime for a group of respondents that has not been studied much before in cybercrime research.

In line with previous research, the results showed that there is a considerable victim-offender overlap for both cybercrime and traditional crime, even for adults and computer-dependent cybercrime. Although the percentage of cybercrime victim-offenders is relatively small, the physical convergence of victims and offenders was not required to observe an overlap. For both cybercrime and traditional crime differences appeared between offenders-only, victims-only and victim-offenders in seriousness of victimization, types of victimization and offending, and the underlying correlates. These findings indicate that research on both cybercrime offending and victimization can benefit from studying offending and victimization in conjunction, while taking into account the differences between offenders-only, victims-only and victim-offenders (Schreck, Stewart, and Wayne Osgood 2008; Van Gelder et al. 2015).

More technical cybercrimes were more common in the offenders-only group than in the group of victim-offenders. This was also reflected in the correlates of offending-only as offenders had IT-skills and specific routine activities that increased their knowledge for more technical offending, but also their ability to protect themselves from being victimized. In contrast, victim-offenders had significantly lower self-control and displayed more general online routine activities. This was in line with previous research on victim-offenders for financial cybercrime (Kerstens and Jansen 2016) and research on offenders that suggests that more technical crimes require more self-control and IT-skills (Holt and Kilger 2008). People who spent more time programming were less likely to be cybercrime victims-only. Those people might have more IT-skills, run less common operating systems and browsers and are less likely to share their computer with others, which reduces their victimization risk. This is supported by the result that malware victimization is the only type of victimization that is more common among victims-only, and these factors are specifically related to malware victimization (Leukfeldt and Yar 2016).

In line with previous research (Berg and Felson 2016; Lauritsen and Laub 2007) we found that traditional victimization-offending was more often related to violence than victimization-only or offending-only. Victimization-only was related to situational factors and the behavior of others, while offenders-only and especially victim-offenders are more at risk because of their own behavior in criminogenic settings. Alcohol abuse was especially related to offending (Schreck, Stewart, and Wayne Osgood 2008) and in line with Van Gelder et al. (2015) low self-control was an important predictor of victimization-offending. Interestingly, online shopping was related to traditional offending-only, possibly because it created opportunities for traditional crimes such as theft and tax fraud which was more common among offenders-only than among victim-offenders.

There were similar patterns of situational and/or personal correlates with offending-only, victimization-only or victimization-offending for both cybercrime and traditional crime. For both, victim-offenders had a serious risk profile, though cybercrime had somewhat different correlates regarding online routines and living situations. Interestingly, living situations which prevented respondents from exposure to traditional crime increased their exposure to cybercrime. Thus opportunities for cybercriminal behavior and risks for victimization emerge in a totally different context, which results in different situational correlates. In contrast, there were no differences in the effects of self-control demonstrating that low self-control is an important risk factor for cybercrime victimization-offending.

Although the sample, analyses, and comparison used in this study are unique in the field of cybercrime, this research also had limitations. First of all, the cross-sectional data did not allow for assessing causal effects between offending and victimization. We could only examine the existence of overlapping risk factors that were correlated to offending and victimization in the preceding twelve months. The results show that there are similarities in the types of risk factors related to cybercrime and traditional victimization-only, offending-only and victimization-offending. This might mean that causal effects found in previous studies for traditional crime will also be found for cybercrime. For instance, Kerstens and Jansen (2016) showed that for financial cybercrime, retaliation as a motivation for offending was more common among victim-offenders than offenders-only. This could suggest that offending is caused by victimization. Future longitudinal studies should include cybercrime offending and victimization questions in their surveys to examine to what extent the victim-offender overlap for cybercrime is causal or affected by overlapping risk factors.

The sample used for this study provided a unique opportunity to find two comparable high risk samples that both originated from the same law enforcement source. This enabled us to study less common and more technical cybercrimes and compare them to traditional crimes. It should, however, be noted that the offenders studied in this research were all suspects of a crime in the past (preceding the twelve-month period of the self-report questions used in this study) and there was enough evidence in their case to send their case to the prosecutor's office. This means that the ability of respondents to avoid the long arm of the law and the prioritization of the Dutch police influenced who was invited to participate in this study, which may have led to selection bias. In addition, the non-response analyses showed that females were overrepresented among cybercrime respondents and younger people were overrepresented among traditional respondents. Furthermore, this sample is based on Dutch suspects, while some argue that especially the more technically skilled cybercrime offenders originate from other countries (Chua and Holt 2016; European Cybercrime Center 2014; Holt and Kilger 2012). Hence, caution is advised when generalizing the results of this study to the whole population of offenders or to other countries. We did try to avoid selection bias caused by the online survey method, by offering the option to participate through a Tor Hidden Service website or on paper, which was used by a few respondents.

With respect to the validity of the results, it should be noted that just like previous studies of cybercrime, we were not able to rule out the possibility that respondents with more IT-skills are better able to detect that they are victimized. However, victims-only showed less IT-skills than offenders-only and victim-offenders. IT-skills were also not significantly related to victimization-only, while it was related to offending-only and victimization-offending. In combination with the

negative effect of programming on victimization-only, this suggests that victims-only have less IT-skills and are less capable of protecting themselves from being victimized. This might mean that the positive effect of IT-skills on victimization found in previous literature was actually the result of risky online routine activities and maybe even offending of people with more IT-skills.

The combination of online and offline routines, self-control and background characteristics was better able to explain the difference between offending-only, victimization-only, and victimization-offending for cybercrime than for traditional crime. This indicates that when traditional explanations of victimization and offending are updated to the digital context and studied in conjunction with their traditional counterparts, we are even better able to explain the differences between cybercrime victims-only, offenders-only and victim-offenders than we are for traditional crime. Future studies should therefore include both online and offline offending and victimization and look at a combination of traditional explanations and new explanations for cybercrime. Future studies should also further examine which exact situational and personal characteristics are related to cybercrime victimization-offending. As the initial group variable (cybercrime or traditional suspect) still significantly predicted who was a cybercrime victim-offender, this suggests that there are even more situational or personal characteristics that increase their risk for both offending and victimization for cybercrime. Future studies should further investigate the exact personal and situational factors involved, ideally in a design that objectively measures digital behavior.

In sum, this empirical comparison of risk factors related to both cybercrime and traditional victimization-only, offending-only and victimization-offending offered insights into the very different context in which these crimes take place. It showed that in addition to victims-only and offenders-only there is a victim-offender overlap for cybercrime and this could, at least partially, be the result of overlapping risk factors that are related to the digital context in which both offending and victimization of cybercrime takes place.

Declaration of interest

The Author(s) declare(s) that there is no conflict of interest

Notes on contributors

Marleen Weulen Kranenbarg wrote her PhD dissertation at the Netherlands Institute for the Study of Crime and Law Enforcement (NSCR). Her research focuses on perpetrators of cybercrime in comparison to perpetrators of other crime. Currently, she works as an assistant professor at the Department of Criminology of the Vrije Universiteit Amsterdam, The Netherlands.

Dr. *Thomas J. Holt* is a Professor in the School of Criminal Justice at Michigan State University. He received his PhD in 2005 from the University of Missouri Saint Louis. His research focuses on cybercrime, deviance, cyberterrorism, and the law enforcement response to these offenses.

Jean-Louis van Gelder is a senior researcher at the Netherlands Institute for the Study of Crime and Law Enforcement (NSCR). His current research interests include criminal decision making, affect and cognition, personality, the victim–offender overlap, multiple self models, and novel research methods.

ORCID

Marleen Weulen Kranenbarg http://orcid.org/0000-0001-7217-5166

References

Averdijk, Margit, Jean-Louis Van Gelder, Manuel Eisner, and Denis Ribeaud. 2016. "Violence Begets Violence… but How? A Decision-Making Perspective on the Victim-Offender Overlap." *Criminology* 54(2):282–306. doi:10.1111/1745-9125.12102.

Berg, Mark T. and Richard B. Felson. 2016. "Why Are Offenders Victimized So Often?" Pp. 49–65 in *The Wiley Handbook on the Psychology of Violence*, edited by C. A. Cuevas, C. M. Rennison. John Wiley, and Ltd. Sons. West Sussex, UK.

Berg, Mark T., Eric A. Stewart, Christopher J. Schreck, and Ronald L. Simons. 2012. "The Victim–Offender Overlap in Context: Examining the Role of Neighborhood Street Culture." *Criminology* 50(2):359–90. doi:10.1111/j.1745-9125.2011.00265.x.

Bernasco, Wim, Stijn Ruiter, Gerben J. N. Bruinsma, Lieven J. R Pauwels, and Frank M. Weerman. 2013. "Situational Causes of Offending: A Fixed-Effects Analysis of Space–Time Budget Data." *Criminology* 51(4):895–926. doi:10.1111/1745-9125.12023.

Blackburn, J., N. Kourtellis, J. Skvoretz, M. Ripeanu, and A. Iamnitchi. 2014. "Cheating in Online Games: A Social Network Perspective." *Acm Transactions on Internet Technology* 13(3):1–25. doi:10.1145/2630790.

Blokland, Arjan A. J. 2014. "School, Intensive Work, Excessive Alcohol Use and Delinquency during Emerging Adulthood." Pp. 87–107 in *Criminal Behaviour from School to the Workplace: Untangling the Complex Relations between Employment, Education and Crime*, edited by F. M. Weerman and C. Bijleveld. New York: Routledge.

Bossler, Adam M. and George W. Burruss. 2011. "The General Theory of Crime and Computer Hacking: Low Self-Control Hackers?" Pp. 38–67 in *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications*, edited by T. J. Holt and B. H. Schell. New York: Information Science Reference.

Bossler, Adam M. and Thomas J. Holt. 2009. "On-Line Activities, Guardianship, and Malware Infection: An Examination of Routine Activities Theory." *International Journal of Cyber Criminology* 3(1):400–20.

Bossler, Adam M. and Thomas J. Holt. 2010. "The Effect of Self-Control on Victimization in the Cyberworld." *Journal of Criminal Justice* 38(3):227–36. doi:10.1016/j.jcrimjus.2010.03.001.

Choi, Kyung-shick. 2008. "Computer Crime Victimization and Integrated Theory: An Empirical Assessment." *International Journal of Cyber Criminology* 2(1):308.

Chua, Yi-Ting and Thomas J. Holt. 2016. "A Cross-National Examination of the Techniques of Neutralization to Account for Hacking Behaviors." *Victims & Offenders* 11(4):534–55. doi:10.1080/15564886.2015.1121944.

De Vries, Reinout E. and Marise PH Born. 2013. "De Vereenvoudigde Hexaco Persoonlijkheidsvragenlijst En Een Additioneel Interstitieel Proactiviteitsfacet." *Gedrag & Organisatie* 26(2):223–45.

Dirkzwager, Anja J. E. and Paul Nieuwbeerta. unpublished. *Prison Project: Codebook and Documentation-D1 Interview*. Leiden/Amsterdam, The Netherlands: Leiden University/NSCR.

Domenie, Miranda M.L., Eric Rutger Leukfeldt, Johan A. Van Wilsem, Jurjen Jansen, and PH. Stol Wouter. 2013. *Slachtofferschap in Een Gedigitaliseerde Samenleving*. Den Haag: Boom Lemma.

European Cybercrime Center. 2014. *The Internet Organized Crime Threat Assessment (Iocta)*. The Hague, The Netherlands: European Police Office (Europol).

Gottfredson, Michael R and Travis Hirschi. 1990. *A General Theory of Crime*. Palo Alto, CA: Stanford University Press.

Grasmick, Harold G., Charles R. Tittle, Robert J. Bursik, and Bruce J. Arneklev. 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. doi:10.1177/0022427893030001002.

Hay, Carter and Michelle M. Evans. 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.

Holt, Thomas J. and Adam M. Bossler. 2008. "Examining the Applicability of Lifestyle-Routine Activities Theory for Cybercrime Victimization." *Deviant Behavior* 30(1):1–25. doi:10.1080/01639620701876577.

Holt, Thomas J. and Adam M. Bossler. 2014. "An Assessment of the Current State of Cybercrime Scholarship." *Deviant Behavior* 35(1):20–40. doi:10.1080/01639625.2013.822209.

Holt, Thomas J., Adam M. Bossler, and David C May. 2012a. "Low Self-Control, Deviant Peer Associations, and Juvenile Cyberdeviance." *American Journal of Criminal Justice* 37(3):378–95. doi:10.1007/s12103-011-9117-3.

Holt, Thomas J. and Max Kilger. 2008. "Techcrafters and Makecrafters: A Comparison of Two Populations of Hackers." Pp. 67–78 in *WOMBAT Workshop on Information Security Threats Data Collection and Sharing, 2008. Silvia Ceballos. WISTDCS'08*. Amsterdam: IEEE computer society.

Holt, Thomas J. and Max Kilger. 2012, "Know Your Enemy: The Social Dynamics of Hacking" *The Honeynet Project* Retrieved (https://honeynet.org/papers/socialdynamics).

Holt, Thomas J., Deborah Strumsky, Olga Smirnova, and Max Kilger. 2012b. "Examining the Social Networks of Malware Writers and Hackers." *International Journal of Cyber Criminology* 6(1):891–903.

Holtfreter, Kristy, Michael D. Reisig, and Travis C. Pratt. 2008. "Low Self-Control, Routine Activities, and Fraud Victimization." *Criminology* 46(1):189–220. doi:10.1111/j.1745-9125.2008.00101.x.

Hu, Qing, Xu Zhengchuan, and Ali Alper Yayla. 2013. "Why College Students Commit Computer Hacks: Insights from a Cross Culture Analysis." in *Pacific Asia Conference on Information Systems (PACIS)*. Jeju Island, Korea.

Hutchings, Alice. 2014. "Crime from the Keyboard: Organised Cybercrime, Co-Offending, Initiation and Knowledge Transmission." *Crime Law and Social Change* 62(1):1–20. doi:10.1007/s10611-014-9520-z.

Jennings, Wesley G., George E. Higgins, Richard Tewksbury, Angela R. Gover, and Alex R. Piquero. 2010. "A Longitudinal Assessment of the Victim-Offender Overlap." *Journal of Interpersonal Violence* 25(12):2147–74. doi:10.1177/0886260509354888.

Jennings, Wesley G., Alex R. Piquero, and Jennifer M. Reingle. 2012. "On the Overlap between Victimization and Offending: A Review of the Literature." *Aggression and Violent Behavior* 17(1):16–26. doi:10.1016/j.avb.2011.09.003.

Jensen, Gary F and David Brownfield. 1986. "Gender, Lifestyles, and Victimization: Beyond Routine Activity." *Violence and Victims* 1(2):85–99.

Kerstens, Joyce and Jurjen Jansen. 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. doi:10.1080/01639625.2015.1060796.

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

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

Leukfeldt, Eric Rutger. 2014. "Phishing for Suitable Targets in the Netherlands: Routine Activity Theory and Phishing Victimization." *Cyberpsychology Behavior and Social Networking* 17(8):551–55. doi:10.1089/cyber.2014.0008.

Leukfeldt, Eric Rutger and Majid Yar. 2016. "Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis." *Deviant Behavior* 37(3):263–80. doi:10.1080/01639625.2015.1012409.

Longshore, Douglas, Eunice Chang, Shih-chao Hsieh, and Nena Messina. 2004. "Self-Control and Social Bonds: A Combined Control Perspective on Deviance." *Crime & Delinquency* 50(4):542–64. doi:10.1177/0011128703260684.

Morris, R.G. 2011. "Computer Hacking and the Techniques of Neutralization: An Empirical Assessment." Pp. 1–17 in *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications*, edited by T. J. Holt and B. H. Schell. New York: Information Science Reference.

National Cyber Security Centre. 2012. *Cybercrime: From Recognition to Report [Cybercrime. Van Herkenning Tot Aangifte]*. The Hague, The Netherlands: NCSC [Nationaal Cyber Security Centrum], Ministry of Security and Justice.

Netherlands, Statistics. 2014. *Safetymonitor 2014 [Veiligheidsmonitor 2014]*. The Hague, The Netherlands: Statistics Netherlands.

Ngo, Fawn T and Raymond Paternoster. 2011. "Cybercrime Victimization: An Examination of Individual and Situational Level Factors." *International Journal of Cyber Criminology* 5(1):773–93.

Office for National Statistics. 2015. "Improving Crime Statistics in England and Wales." *Crime Statistics, Year Ending June 2015 Release*. Retrieved February 19, 2016 (http://webarchive.nationalarchives.gov.uk/20160105160709/http://www.ons.gov.uk/ons/rel/crime-stats/crime-statistics/year-ending-june-2015/sty-fraud.html).

Ousey, Graham C., Pamela Wilcox, and Bonnie S. Fisher. 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, Alex R., John MacDonald, Adam Dobrin, Leah E. Daigle, and Francis T. Cullen. 2005. "Self-Control, Violent Offending, and Homicide Victimization: Assessing the General Theory of Crime." *Journal of Quantitative Criminology* 21(1):55–71. doi:10.1007/s10940-004-1787-2.

Pontell, H. and S. Rosoff. 2009. "White-Collar Delinquency." *Crime Law and Social Change* 51(1):147–62. doi:10.1007/s10611-008-9146-0.

Pratt, Travis C., Jillian J. Turanovic, Kathleen A. Fox, and Kevin A. Wright. 2014. "Self-Control and Victimization: A Meta-Analysis." *Criminology* 52(1):87–116. doi:10.1111/1745-9125.12030.

Rogers, M. 2001. *A Social Learning Theory and Moral Disengagement Analysis of Criminal Computer Behavior: An Exploratory Study*. University of Manitoba.

Sampson, Robert J. and Janet L. Lauritsen. 1990. "Deviant Lifestyles, Proximity to Crime, and the Offender-Victim Link in Personal Violence." *Journal of Research in Crime and Delinquency* 27(2):110–39. doi:10.1177/0022427890027002002.

Schreck, Christopher J. 1999. "Criminal Victimization and Low Self-Control: An Extension and Test of a General Theory of Crime." *Justice Quarterly* 16(3):633–54. doi:10.1080/07418829900094291.

Schreck, Christopher J., Eric A. Stewart, and Bonnie S. Fisher. 2006. "Self-Control, Victimization, and Their Influence on Risky Lifestyles: A Longitudinal Analysis Using Panel Data." *Journal of Quantitative Criminology* 22(4):319–40. doi:10.1007/s10940-006-9014-y.

Schreck, Christopher J., Eric A. Stewart, and D. Wayne Osgood. 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, Christopher J., Richard A. Wright, and J. Mitchell Miller. 2002. "A Study of Individual and Situational Antecedents of Violent Victimization." *Justice Quarterly* 19(1):159–80. doi:10.1080/07418820200095201.

Suler, John. 2004. "The Online Disinhibition Effect." *CyberPsychology & Behavior* 7(3):321–26. doi:10.1089/1094931041291295.

Svensson, Robert, Frank M. Weerman, J. R. Lieven, Gerben J. Pauwels, N. Bruinsma, and Wim Bernasco. 2013. "Moral Emotions and Offending: Do Feelings of Anticipated Shame and Guilt Mediate the Effect of Socialization on Offending?." *European Journal of Criminology* 10(1):22–39. doi:10.1177/1477370812454393.

Tcherni, M., A. Davies, G. Lopes, and A. Lizotte. 2016. "The Dark Figure of Online Property Crime: Is Cyberspace Hiding a Crime Wave?." *Justice Quarterly* 33(5):890–911. doi:10.1080/07418825.2014.994658.

Turanovic, Jillian J. and Travis C. Pratt. 2013. "The Consequences of Maladaptive Coping: Integrating General Strain and Self-Control Theories to Specify a Causal Pathway between Victimization and Offending." *Journal of Quantitative Criminology* 29(3):321–45. doi:10.1007/s10940-012-9180-z.

Van Gelder, Jean-Louis, Margit Averdijk, Manuel Eisner, and Denis Ribeaud. 2015. "Unpacking the Victim-Offender Overlap: On Role Differentiation and Socio-Psychological Characteristics." *Journal of Quantitative Criminology* 31 (4):653–75. doi:10.1007/s10940-014-9244-3.

Van Gelder, Jean-Louis and Reinout E. De Vries. 2012. "Traits and States: Integrating Personality and Affect into a Model of Criminal Decision Making." *Criminology* 50(3):637–71. doi:10.1111/j.1745-9125.2012.00276.x.

Van Wilsem, Johan A. 2013. "Hacking and Harassment—Do They Have Something in Common? Comparing Risk Factors for Online Victimization." *Journal of Contemporary Criminal Justice* 29(4):437–53. doi:10.1177/1043986213507402.

Wall, David S. 2001. "Cybercrimes and the Internet." Pp. 1–17 in *Crime and the Internet*. London: Routledge.

Weesie, Jeroen. 1999. "Sg21: Seemingly Unrelated Estimation and the Cluster-Adjusted Sandwich Estimator." *Stata Technical Bulletin* 52:34–47.

Wolfe, Scott E., George E. Higgins, and Catherine D. Marcum. 2008. "Deterrence and Digital Piracy: A Preliminary Examination of the Role of Viruses." *Social Science Computer Review* 26(3):317–33. doi:10.1177/0894439307309465.

Yar, Majid. 2005. "The Novelty of 'Cybercrime'. An Assessment in Light of Routine Activity Theory." *European Journal of Criminology* 2(4):407–27. doi:10.1177/147737080556056.