Cyber-offenders versus traditional offenders

An empirical comparison

Marleen Weulen Kranenburg
Chapter 3

Offending and victimisation in the digital age: comparing correlates of cybercrime and traditional offending-only, victimisation-only and the victimisation-offending overlap*

* This chapter was accepted for publication as: Weulen Kranenbarg, M., Holt, T.J., & Van Gelder, J.L. (forthcoming). Offending and victimization in the digital age: comparing correlates of cybercrime and traditional offending-only, victimization-only and the victimization-offending overlap. Deviant Behavior.
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 for cybercrime these risk factors may not be similar to risk factors for traditional crime. Utilizing a high risk sample of cyber-dependent offenders and traditional offenders ($N=535$) we compare victimisation, offending, and victimisation-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 victimisation, offending, and victimisation-offending. Some cybercrime correlates are related to the digital context, but show similar patterns for cybercrime and traditional crime.

Keywords

cybercrime
victim-offender overlap
comparison
traditional crime
shared risk factors
3.1 Introduction

Recent research demonstrates that over the last two decades there has been a significant rise in the rate of crimes that utilise Information Technology (IT) systems, 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’ (p. 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 & Holt, 2009; Holt & Bossler, 2008; Kerstens & Jansen, 2016; Suler, 2004; Yar, 2005a). This raises the question as to whether traditional correlates of offending and victimisation can account for cybercrime offending and victimisation.

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 victimised (e.g., Averdijk et al., 2016; Berg et al., 2012; Hay & Evans, 2006; Lauritsen & Laub, 2007; Lauritsen et al., 1991; Ousey et al., 2011; Rokven et al., 2017; Rokven et al., 2016; Schreck et al., 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 victimisation. In addition, offending can directly cause victimisation or vice versa (for a review, see Berg & Felson, 2016; Jennings et al., 2012; Lauritsen & Laub, 2007). It should be noted that only a part of the offender population is at risk of victimisation, and not all victims commit crimes. Therefore scholars recently stressed the importance of studying victims-only, offenders-only, and victim-offenders as separate groups to clearly identify any differences in underlying risk factors (e.g., Schreck et al., 2008; Van Gelder et al., 2015).

Although cybercrime offending and victimisation 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 & Bossler, 2014). In fact, cybercrime offending has been found to be a risk factor for victimisation and vice versa (e.g., Bossler & Holt, 2009; Morris, 2001; Ngo & Paternoster, 2011; Wolfe et al., 2008). This indicates that cybercrime offending and victimisation 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 & Jansen, 2016). This study found a considerable crossover in financial cybercrime offending and victimisation which was associated with low self-control, retaliation, high online disinhibition, and online routine activities (Kerstens & 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 victimisation. The risk factors for offending and victimisation are compared within offending-only, victimisation-only and victimisation-offending groups, for technical cyber-dependent crime (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 victimisation in a way similar to traditional crime.

### 3.1.1 Risk factors for traditional crime and cybercrime

Personal and situational risk factors such as low self-control, risky life-styles or routine activities, substance abuse and socioeconomic status are associated with both offending and victimisation risks for traditional crimes (e.g., Berg & Felson, 2016; Jennings et al., 2012; Rokven et al., 2016). People, who spend more time with delinquent friends and/or in places where crimes take place, are more at risk of being victimised and also have more criminal opportunities (e.g., Jensen & Brownfield, 1986; Lauritsen et al., 1991; Rokven et al., 2016; Sampson & Lauritsen, 1990; Schreck, Wright, & Miller, 2002). In addition, impulsivity and low self-control can directly increase victimisation and offending (e.g., Gottfredson & Hirschi, 1990; Jennings, Higgins, Tewksbury, Gover, & Piquero, 2010; Piquero, MacDonald, Dobrin, Daigle, & Cullen, 2005; Pratt, Turanovic, Fox, & Wright, 2014), but also indirectly through the association between low self-control and increased time spent in criminogenic settings (e.g., Schreck, 1999; Schreck, Stewart, & Fisher, 2006). Similarly, substance abuse is a clear risk factor for traditional victimisation and offending (e.g., Berg & Felson, 2016; Longshore, Chang, Hsieh, & Messina, 2004; Turanovic & 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 victimisation. The relationship between traditional offending and victimisation is the strongest for violent crimes, which per definition require physical interaction between victims and offenders (Berg & Felson, 2016; Lauritsen & Laub, 2007). In the case of cybercrime there is no physical convergence in space and time of offenders and victims (e.g., Bossler & Holt, 2009; Holt & Bossler, 2008; Yar, 2005a). 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 victimisation, as well as common risk factors for both experiences, including low self-control, routine activities and socio-demographic characteristics (e.g., Bossler & Holt, 2009; Holt & Bossler, 2014; Ngo & Paternoster, 2011; Wolfe et al., 2008).

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

3.1.2 Assessing the theoretical explanations for the victim-offender overlap

Considering the common risk factors associated with cybercrime victimisation 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 & 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 & Bossler, 2014). These same conditions may increase an individual’s risk of victimisation as savvy offenders may target those who are online more frequently and engage in risky activities like downloading pirated materials (Bossler & Holt, 2010). Empirical
studies on low self-control show mixed results. Van Wilsem (2013) found that low self-control was positively related to hacking victimisation, while Bossler and Holt (2010) found that low self-control was neither related to hacking nor to malware victimisation. Holtfreter, Reisig, and Pratt (2008) found that although targeting of scam victims is random, the personal characteristics and behaviour of the victim influenced who responded to a scam. As a result, low self-control may play a role in the risk of victimisation regardless of the targeted nature of victimisation.

With respect to offending, it has been argued that advanced types of hacking and other technical cyber-dependent crimes 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 & Burruss, 2011). They must also have the patience to plan and execute the offence properly and cover their tracks (e.g., Holt & 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 & Burruss, 2011; Holt, Bossler, et al., 2012). As the current study focuses on these cyber-dependent crimes, low self-control may be less important for cybercrime offending and victimisation compared to traditional crime.

3.1.3 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 victimisation. To that end, several studies have found time spent in specific activities, like time spent using email or social media, increases individual risks of interpersonal victimisation such as online harassment (Bossler & Holt, 2009; Holt & 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 victimisation (Leukfeldt & Yar, 2016). Time spent using the internet, targeted and untargeted browsing, online shopping, downloading and gaming were all related to malware victimisation (Leukfeldt & 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, Strumsky, Smirnova, & Kilger, 2012; Hutchings, 2014). In addition, online gaming environments can increase
opportunities and motivation for hacking, but could consequently also increase the risk for victimisation. An example is hacking into gaming accounts to steal virtual objects or credits (Blackburn, Kourtellis, Skvoretz, Ripeanu, & Iamnitchi, 2014; Hu, Xu, & 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 victimisation.

Studies of cybercrime victimisation 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 et al., 1991). The absence of measures may lead to model misspecification as online activity could increase the risk of offline crimes like fraud (Holtfreter et al., 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 behaviours on the risk of offending and victimisation (Leukfeldt & 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 victimisation 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 & Burruss, 2011; Chua & Holt, 2016; Holt, Bossler, et al., 2012; Holt & Kilger, 2008).

Technological capacity may also serve as a protective factor against cybercrime victimisation, as it is thought technically proficient individuals can identify when their computer may have been compromised or utilise appropriate resources to secure their system. Most studies, however, find no relationship between IT-skills and malware infections (e.g., Bossler & Holt, 2009; Ngo & 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 victimisation. Leukfeldt and Yar (2016) found that although computer knowledge in general was not related to hacking or malware victimisation, operating system and browser type were related to malware victimisation and risk awareness was negatively related to hacking victimisation.
In addition, the link between socio-demographic factors that explain traditional offending and victimisation and cybercrime is mixed. Previous research suggests that cybercrime offending, especially of more cyber-dependent crimes, occurs in higher social classes (e.g., Pontell & Rosoff, 2009) and victimisation occurs more often among higher educated people (e.g., Leukfeldt & Yar, 2016).

### 3.1.4 The current study
To address the issues discussed above, this analysis explores the correlates of offending and victimisation for cyber-dependent crimes like hacking, data theft, and defacing. We test whether the risk factors that have been found to predict cybercrime victimisation and offending separately also explain victimisation-offending, offending-only and victimisation-only. A comparative model is also developed for traditional offences to compare the risk factors between cybercrime and traditional crime.

### 3.2 Data and methods

#### 3.2.1 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 selected from the database of the prosecutor’s office. 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. In the summer of 2015, 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. 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 communication with this type of website is completely encrypted and less easy to trace.
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%, \(\chi^2(1) = 6.10, p < 0.05\)), and for traditional suspects respondents were relatively younger (\(M_{\text{years}} = 38.49\) compared to \(M_{\text{years}} = 40.90\), \(t(1654) = 2.47, p<.05\)).

### 3.2.2 Measures

**Dependent variables**

Victimisation and offending in the preceding twelve 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. Victimisation 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 victimisation. For example, malware victimisation 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 victimisation: 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 victimisation, based on the Dutch Safety Monitor (Statistics Netherlands, 2014c), 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 cyber-dependent crimes 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 …’ 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 victimisation 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 & 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, Tittle, Bursik, and Arneklev (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: 
\[ \text{HEXACO Self-Control} = (3\times\text{Prudence} + 2\times(\text{Fairness + Modesty + Fearfulness + Flexibility}) + (\text{Social Self-esteem + Patience + Inquisitiveness + Diligence + Altruism)})/16. \]
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 3.1.

### Table 3.1.
Descriptive statistics independent variables (N = 459)

<table>
<thead>
<tr>
<th></th>
<th>M</th>
<th>SD</th>
<th></th>
<th>M</th>
<th>SD</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Online routines</strong></td>
<td></td>
<td></td>
<td><strong>Offline routines</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Communication</td>
<td>2.05</td>
<td>1.18</td>
<td>At work</td>
<td>2.81</td>
<td>1.61</td>
</tr>
<tr>
<td>Shopping</td>
<td>0.71</td>
<td>0.69</td>
<td>At school</td>
<td>0.44</td>
<td>1.11</td>
</tr>
<tr>
<td>Gaming</td>
<td>0.83</td>
<td>1.18</td>
<td>At home of friends</td>
<td>1.08</td>
<td>0.71</td>
</tr>
<tr>
<td>Forum use</td>
<td>0.74</td>
<td>0.92</td>
<td>Other with friends</td>
<td>1.18</td>
<td>0.89</td>
</tr>
<tr>
<td>Programming</td>
<td>0.46</td>
<td>1.07</td>
<td>Going out</td>
<td>0.87</td>
<td>0.70</td>
</tr>
<tr>
<td>IT-skills</td>
<td>1.92</td>
<td>1.04</td>
<td>Alcohol abuse</td>
<td>0.25</td>
<td>0.57</td>
</tr>
<tr>
<td>Low self-control</td>
<td>1.73</td>
<td>0.43</td>
<td>Marijuana use</td>
<td>0.38</td>
<td>0.97</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Dummy variables</th>
<th>N</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Male</td>
<td>358</td>
<td>78.00</td>
</tr>
<tr>
<td>Living with family</td>
<td>246</td>
<td>53.59</td>
</tr>
<tr>
<td>Living with parents</td>
<td>80</td>
<td>17.43</td>
</tr>
</tbody>
</table>

**Online routine activities and IT-skills**

Five online routine activities based on the online routines questionnaire of Domenie, Leukfeldt, Van Wilsem, Jansen, and Stol (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, et al. (2012), 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 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 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 & Nieuwbeerta, 2015). 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 ($\alpha = 0.82$). 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).
3.3 Results

3.3.1 Descriptive statistics
For both cybercrime and traditional crime there is a considerable victim-offender overlap. For cybercrime there were 44 victim-offenders, 37 offenders-only, 133 victims-only, and 245 respondents were neither victim nor offender. This means that for cybercrime, victimisation prevalence is 54.32% among offenders and 39.19% among non-offenders. Based on the same numbers but reversely calculated, offending prevalence is 24.86% for victims and 13.12% for non-victims. For traditional crime there were 63 victim-offenders, 31 offenders-only, 140 victims-only, and 225 respondents were neither victim nor offender. Here, victimisation prevalence is 67.02% among offenders and 38.36% among non-offenders, while offending prevalence is 31.03% for victims and 12.11% for non-victims.

When comparing prevalence rates of victimisation and offending between the groups (Table 3.2 and 3.3), both types of victim-offenders experienced statistically significantly more types of victimisation. For cybercrime, only malware victimisation 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 statistically significantly more common among victim-offenders. For offending there is no statistically 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: $\chi^2(1) = 3.01, p = .08$), while hacking in another way is more often committed by offenders-only. Among victim-offenders of traditional crime violence is more common (marginally significant: $\chi^2(1) = 3.18, p = .07$).

---

2 Based again on the same numbers, the relation between victimisation and offending can also be expressed by a single statistic, the odds ratio, which for cybercrime equals $(44 \times 245) / (37 \times 133) = 2.19$, indicating that the odds of victimisation are more than twice as high for offenders as compared to non-offenders.

3 The odds ratio characterizing the association between victimisation and offending in traditional crime is $(63 \times 225) / (31 \times 140) = 3.27$, indicating that the odds of victimisation are more than three times as high for offenders as compared to non-offenders.
Table 3.2.
Prevalence rates victimisation

<table>
<thead>
<tr>
<th>Types of victimisation</th>
<th>Cybercrime victimisation</th>
<th></th>
<th>Traditional victimisation</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Victim-only</td>
<td>%</td>
<td>Victim-offender</td>
<td>%</td>
</tr>
<tr>
<td>Malware</td>
<td>102</td>
<td>76.69</td>
<td>30</td>
<td>68.18</td>
</tr>
<tr>
<td>Hacking</td>
<td>35</td>
<td>26.32</td>
<td>17</td>
<td>38.64</td>
</tr>
<tr>
<td>Data theft/damage</td>
<td>12</td>
<td>9.02</td>
<td>11</td>
<td>25.00**</td>
</tr>
<tr>
<td>Defacing</td>
<td>15</td>
<td>11.28</td>
<td>9</td>
<td>20.45</td>
</tr>
<tr>
<td>DoS</td>
<td>12</td>
<td>9.02</td>
<td>6</td>
<td>13.64</td>
</tr>
<tr>
<td>Phishing</td>
<td>26</td>
<td>19.55</td>
<td>10</td>
<td>22.73</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>M</th>
<th>SD</th>
<th>M</th>
<th>SD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Types of victimisation</td>
<td>1.52</td>
<td>0.96</td>
<td>1.89</td>
</tr>
</tbody>
</table>

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

Table 3.3.
Prevalence rates offending

<table>
<thead>
<tr>
<th>Types of offending</th>
<th>Cybercrime offending</th>
<th></th>
<th>Traditional offending</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Offender-only</td>
<td>N</td>
<td>%</td>
<td>Victim-offender</td>
</tr>
<tr>
<td>Guessing password</td>
<td>9</td>
<td>24.32</td>
<td>16</td>
<td>36.36</td>
</tr>
<tr>
<td>Hacking</td>
<td>13</td>
<td>35.14</td>
<td>8</td>
<td>18.18</td>
</tr>
<tr>
<td>Selling credentials</td>
<td>0</td>
<td>0.00</td>
<td>1</td>
<td>2.27</td>
</tr>
<tr>
<td>Damaging data</td>
<td>7</td>
<td>18.92</td>
<td>9</td>
<td>20.45</td>
</tr>
<tr>
<td>Digital theft</td>
<td>12</td>
<td>32.43</td>
<td>12</td>
<td>27.27</td>
</tr>
<tr>
<td>Selling data</td>
<td>1</td>
<td>2.70</td>
<td>3</td>
<td>6.82</td>
</tr>
<tr>
<td>Malware</td>
<td>3</td>
<td>8.11</td>
<td>6</td>
<td>13.64</td>
</tr>
<tr>
<td>Taking control</td>
<td>8</td>
<td>21.62</td>
<td>7</td>
<td>15.91</td>
</tr>
<tr>
<td>Defacing</td>
<td>12</td>
<td>32.43</td>
<td>14</td>
<td>31.82</td>
</tr>
<tr>
<td>Intercepting comm.</td>
<td>5</td>
<td>13.51</td>
<td>3</td>
<td>6.82</td>
</tr>
<tr>
<td>DoS</td>
<td>1</td>
<td>2.70</td>
<td>4</td>
<td>9.09</td>
</tr>
<tr>
<td>Phishing</td>
<td>6</td>
<td>16.22</td>
<td>7</td>
<td>15.91</td>
</tr>
<tr>
<td>Spam</td>
<td>1</td>
<td>2.70</td>
<td>3</td>
<td>6.82</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>M</th>
<th>SD</th>
<th>M</th>
<th>SD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Types of offending</td>
<td>2.11</td>
<td>1.54</td>
<td>2.11</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>M</th>
<th>SD</th>
<th>M</th>
<th>SD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Types of offending</td>
<td>1.61</td>
<td>0.95</td>
<td>2.05</td>
</tr>
</tbody>
</table>

64
3.3.2 Multinomial analyses

This section will first discuss the results for cybercrime and traditional crime separately and then compare those results. Table 3.4 shows the results from the multinomial logit analyses for cybercrime and traditional crime and the comparison between them. The reference category for both types of crime is being neither victim nor offender. 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. A one-unit increase in low self-control increases the risk of being a victim-offender by a factor of 1.43 compared to being neither a cybercrime victim nor an offender. This estimate is statistically significantly stronger compared to victims-only ($\chi^2(1) = 7.42, p < .01$) and offenders-only ($\chi^2(1) = 4.95, p < .05$). In addition, having more IT-skills and spending more time on online shopping also increases the likelihood of victimisation-offending. The effect of online shopping is statistically significantly stronger compared to offenders-only and victims-only ($\chi^2(1) = 3.88, p < .05$ and $\chi^2(1) = 6.69, p < .05$). In addition, the effect of online communication is stronger for victim-offenders compared to offenders-only ($\chi^2(1) = 4.33, p < .05$). Living with parents and being in the initial group of cybercrime suspects is also positively related to cybercrime victimisation-offending. The effect of living with parents is even in the opposite direction for offenders-only and that difference is statistically significant ($\chi^2(1) = 5.81, p < .05$).

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 statistically significantly from the effect for victim-offenders and victims-only ($\chi^2(1) = 8.58, p < .01$ and $\chi^2(1) = 7.97, p < .01$, respectively). Those effects are in the opposite direction. More IT-skills also statistically significantly increase the likelihood of victimisation-offending, but it is stronger for offending-only. Compared to being neither a victim nor an offender, a one-unit increase in IT-skills increases the risk for being offender-only by a factor of 1.89 while it increases the risk of being a victim-offender by a factor of 1.66. Victims-only spent statistically 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.
### Table 3.4.
Multinomial logit models and between model comparisons

<table>
<thead>
<tr>
<th></th>
<th>Cybercrime¹</th>
<th>Traditional crime²</th>
<th>Model comparisons³</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Offender-only</td>
<td>Victim-only</td>
<td>Victim-Offender</td>
</tr>
<tr>
<td>Low self-control</td>
<td>1.43 (0.68)</td>
<td>1.31 (0.37)</td>
<td>4.05 (1.91)**</td>
</tr>
<tr>
<td>Online routines</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Communication</td>
<td>0.74 (0.14)</td>
<td>1.21 (0.13)</td>
<td>1.17 (0.20)</td>
</tr>
<tr>
<td>Shopping</td>
<td>0.82 (0.28)</td>
<td>0.82 (0.16)</td>
<td>1.75 (0.46)*</td>
</tr>
<tr>
<td>Gaming</td>
<td>1.06 (0.18)</td>
<td>1.15 (0.13)</td>
<td>1.22 (0.20)</td>
</tr>
<tr>
<td>Forum use</td>
<td>1.60 (0.35*)</td>
<td>0.83 (0.12)</td>
<td>0.64 (0.15)</td>
</tr>
<tr>
<td>Programming</td>
<td>0.97 (0.18)</td>
<td>0.67 (0.11*)</td>
<td>0.83 (0.17)</td>
</tr>
<tr>
<td>IT-skills</td>
<td>1.89 (0.48*)</td>
<td>1.23 (0.19)</td>
<td>1.66 (0.41*)</td>
</tr>
<tr>
<td>Offline routines</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>At work</td>
<td>1.03 (0.33)</td>
<td>1.37 (0.26)</td>
<td>1.58 (0.45)</td>
</tr>
<tr>
<td>At school</td>
<td>1.39 (0.39)</td>
<td>1.08 (0.19)</td>
<td>1.38 (0.35)</td>
</tr>
<tr>
<td>At home of friends</td>
<td>1.26 (0.19)</td>
<td>1.04 (0.08)</td>
<td>1.06 (0.14)</td>
</tr>
<tr>
<td>Other with friends</td>
<td>1.07 (0.18)</td>
<td>0.96 (0.13)</td>
<td>0.92 (0.16)</td>
</tr>
<tr>
<td>Going out</td>
<td>1.48 (0.48)</td>
<td>0.85 (0.17)</td>
<td>0.86 (0.26)</td>
</tr>
<tr>
<td>Alcohol abuse</td>
<td>0.83 (0.29)</td>
<td>0.83 (0.19)</td>
<td>1.33 (0.38)</td>
</tr>
<tr>
<td>Marijuana use</td>
<td>1.19 (0.22)</td>
<td>1.21 (0.16)</td>
<td>1.39 (0.25)</td>
</tr>
</tbody>
</table>
Table 3.4. Continued

<table>
<thead>
<tr>
<th>Background characteristics</th>
<th>Male</th>
<th>Age</th>
<th>Living with family</th>
<th>Living with parents</th>
<th>Financial situation</th>
<th>Initial group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Male</td>
<td>0.34</td>
<td>0.99</td>
<td>0.44</td>
<td>0.60</td>
<td>3.53</td>
<td>1.83</td>
</tr>
<tr>
<td>Age</td>
<td>0.19</td>
<td>0.02</td>
<td>0.21</td>
<td>0.35</td>
<td>2.62</td>
<td>0.85</td>
</tr>
<tr>
<td>Living with family</td>
<td>1.07</td>
<td>0.99</td>
<td>1.91</td>
<td>1.74</td>
<td>1.35</td>
<td>1.29</td>
</tr>
<tr>
<td>Living with parents</td>
<td>0.31</td>
<td>0.01</td>
<td>0.57*</td>
<td>0.69</td>
<td>0.62</td>
<td>0.32</td>
</tr>
<tr>
<td>Financial situation</td>
<td>0.88</td>
<td>0.99</td>
<td>1.55*</td>
<td>3.26</td>
<td>1.63</td>
<td>2.41</td>
</tr>
<tr>
<td>Initial group</td>
<td>0.44</td>
<td>0.98</td>
<td>0.74</td>
<td>0.28</td>
<td>1.50</td>
<td>1.15</td>
</tr>
</tbody>
</table>

| Combined comparison         | 37   | 133 | 44     | 31   | 140 | 63  |

| LR $\chi^2$ (60) = 127.73; Reference group is: neither victim nor offender cybercrime (N = 245) |
| LR $\chi^2$ (60) = 118.33; Reference group is: neither victim nor offender traditional crime (N = 225) |
| This table only includes between model comparisons of cybercrime and traditional crime. Statistically 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. |

* p<.05; ** p<.01; *** p<.001 (two-tailed)
Traditional crime

Alcohol abuse is statistically significantly related to both offending and victimisation-offending, while going out is related to victimisation-only but not to the other two. The effects of going out and alcohol abuse also differ statistically significantly between offenders-only and victims-only ($\chi^2(1) = 6.11, p < .05$ and $\chi^2(1) = 4.61, p < .05$). For victim-offenders there is also a statistically significant effect of low self-control and spending more time outside with friends. The effect of spending time outside with friends also differs statistically significantly between victims-only and victim-offenders ($\chi^2(1) = 6.08, p < .05$). There are no statistically 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 the risk for victimisation-only, while marijuana use, living with parents and age are negatively related to victimisation-only. The effect of marijuana use is in the opposite direction for victim-offenders and that difference is statistically significant ($\chi^2(1) = 9.27, p < .01$). Lastly, victim-offenders report more financial problems. The effects of alcohol abuse, online shopping, and programming differ statistically significantly between offenders-only and victims-only ($\chi^2(1) = 4.61, p < .05$; $\chi^2(1) = 5.09, p < .05$; $\chi^2(1) = 9.31, p < .01$). 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 statistically significantly different between cybercrime and traditional crime, for offenders-only, victims-only and victim-offenders. The combined effects of online routines are statistically significantly different between offenders-only and victim-offenders, while the combined effects of the background characteristics are statistically 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, victimisation-only and victimisation-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 statistically significantly between both groups of victims-only, the differences in the living situations are important. For offenders-only the effect of programming differs statistically significantly. Where programming statistically significantly reduces traditional offending it cannot reduce cybercrime offending. As the overall effect of online routines is also statistically significantly different, cybercrime offenders-only are very different from traditional offenders-only in their online behaviour and IT-skills. For victim-offenders the effects of IT-skills and living with parents differ statistically significantly. Living with parents is marginally significant for traditional offenders, \( p = .09 \). Overall, the most striking difference can be found in online routine activities, IT-skills and living situations.

### 3.4 Conclusion and 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, victimisation-only and victimisation-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 cyber-dependent crime 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 cyber-dependent crime. 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 victimisation, types of victimisation and offending, and the underlying correlates. These findings indicate that research on both cybercrime offending and victimisation can benefit from studying offending and victimisation in conjunction, while taking into account the differences between offenders-only, victims-only and victim-offenders (Schreck et al., 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 victimised. In contrast, victim-offenders had statistically 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 & Jansen, 2016) and research on offenders that suggests that more technical crimes require more self-control and IT-skills (Holt & 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 victimisation risk. This is supported by the result that malware victimisation is the only type of victimisation that is more common among victims-only, and these factors are specifically related to malware victimisation (Leukfeldt & Yar, 2016).

In line with previous research (Berg & Felson, 2016; Lauritsen & Laub, 2007) we found that traditional victimisation-offending was more often related to violence than victimisation-only or offending-only. Victimisation-only was related to situational factors and the behaviour of others, while offenders-only and especially victim-offenders are more at risk because of their own behaviour in criminogenic settings. Alcohol abuse was especially related to offending (Schreck et al., 2008) and in line with Van Gelder et al. (2015) low self-control was an important predictor of victimisation-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, victimisation-only or victimisation-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 behaviour and risks for victimisation 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 victimisation-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 victimisation. We could only examine the existence of overlapping risk factors that were correlated to offending and victimisation in the preceding twelve months. The results show that there are similarities in the types of risk factors related to cybercrime and traditional victimisation-only, offending-only and victimisation-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 victimisation. Future longitudinal studies could include cybercrime offending and victimisation 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 people who have never been registered as a suspect of a crime were excluded from this study. Consequently, the ability of offenders to avoid the long arm of the law and the prioritisation 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 & Holt, 2016; European Cybercrime Center, 2014; Holt & 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 victimised. However, victims-only showed less IT-skills than offenders-only and victim-offenders. IT-skills were also not statistically significantly related to victimisation-only, while it was related to offending-only and victimisation-offending. In combination with the negative effect of programming on victimisation-only, this suggests that victims-only have less IT-skills and are less capable of protecting themselves from being victimised. This might mean that the positive effect of IT-skills on victimisation 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, victimisation-only and victimisation-offending for cybercrime than for traditional crime. This indicates that when traditional explanations for victimisation 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 could therefore include both online and offline offending and victimisation and look at a combination of traditional explanations and new explanations for cybercrime. Future studies could also further examine which exact situational and personal characteristics are related to cybercrime victimisation-offending. As the initial group variable (cybercrime or traditional suspect) still statistically 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 victimisation for cybercrime. Future studies could further investigate the exact personal and situational factors involved, ideally in a design that objectively measures digital behaviour.

In sum, this empirical comparison of risk factors related to both cybercrime and traditional victimisation-only, offending-only and victimisation-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 victimisation of cybercrime takes place.
References


References


References


