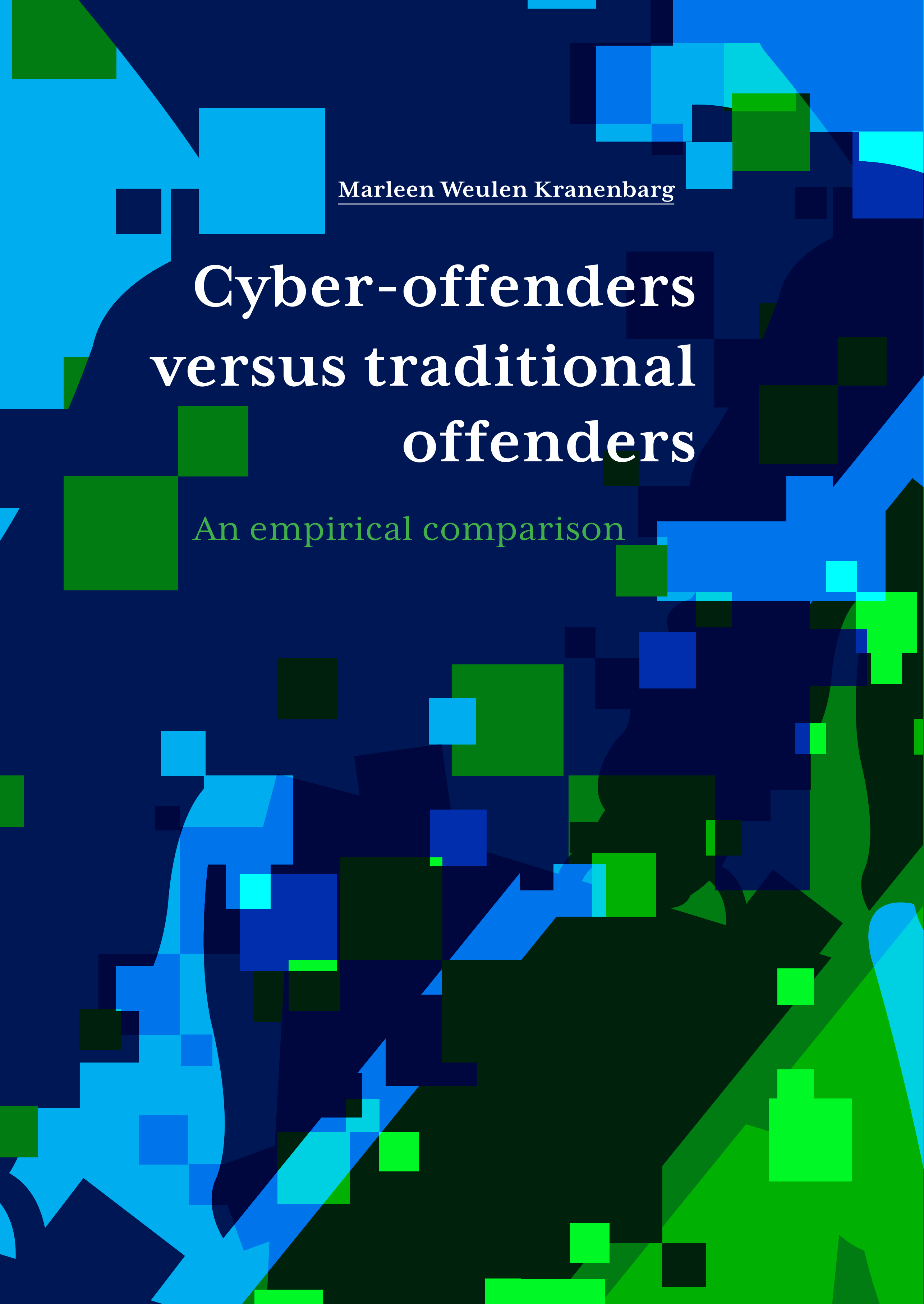


Marleen Weulen Kranenbarg

Cyber-offenders versus traditional offenders

An empirical comparison

Cyber-offenders versus traditional offenders
An empirical comparison

Marleen Weulen Kranenbarg

ISBN: 978-94-92801-18-0

Design and print: proefschrift-aio.nl

This research was supported by the Netherlands Organisation for Scientific Research (NWO) in the framework of the Cyber Security research program under Grant 12-NROI-058b.

VRIJE UNIVERSITEIT

Cyber-offenders versus traditional offenders
An empirical comparison

ACADEMISCH PROEFSCHRIFT

ter verkrijging van de graad Doctor aan
de Vrije Universiteit Amsterdam,
op gezag van de rector magnificus
prof.dr. V. Subramaniam,
in het openbaar te verdedigen
ten overstaan van de promotiecommissie
van de Faculteit der Rechtsgeleerdheid
op vrijdag 26 januari 2018 om 13.45 uur
in de aula van de universiteit,
De Boelelaan 1105

door
Marleen Weulen Kranenbarg
geboren te Apeldoorn

promotoren:	prof.dr. W. Bernasco
	prof.dr. S. Ruiter
copromotor:	dr. J.L. van Gelder

manuscript committee:

prof.dr. E.R. Kleemans, *Vrije Universiteit Amsterdam*
prof.dr. A.R. Lodder, *Vrije Universiteit Amsterdam*
prof.dr. F. Miró-Llinares, *Universidad Miguel Hernandez De Elche*
prof.dr. F.M. Weerman, *Erasmus Universiteit Rotterdam*
dr. J.A. van Wilsem, *Wetenschappelijk Onderzoek- en Documentatiecentrum*

Table of contents

Chapter 1

General introduction

1.1 Introduction

For the past two decades, estimates show a dramatic increase in the percentage of the world population that is connected to the internet. In 1995, less than 1% of the world population was connected, while estimates show that in 2016 the internet penetration rate was approximately 46% and nowadays every minute approximately 525 new people are connected to the internet. In the Netherlands, the internet penetration rate is even much higher, namely 94% (Internet Live Stats, 2017). This increased connectivity and use of Information Technology (IT) has provided many new legitimate opportunities, for example for communication and information exchange, but it has also created new opportunities for committing crimes. These criminal opportunities are reflected in the finding that, in contrast to the decrease in the prevalence of traditional crime (Tonry, 2014), the prevalence of cybercrime is increasing (e.g., Brady, Randa, & Reyns, 2016; Grabosky, 2017; Tcherni, Davies, Lopes, & Lizotte, 2016; White, 2013).

1.2 Cybercrime

Within the broad range of cybercrimes, the literature generally distinguishes between (A) traditional crimes for which IT is in some form used in its commission and (B) new forms of crime that target IT and in which IT is key in the commission of the crime (e.g., Furnell, 2002; Gordon & Ford, 2006; McGuire & Dowling, 2013; Wall, 2001; Zhang, Xiao, Ghaboosi, Zhang, & Deng, 2012). The traditional crimes (A) will be called *cyber-enabled crimes* in this dissertation and the new forms of crime (B) will be called *cyber-dependent crimes*. Cyber-enabled crimes are crimes like online fraud, stalking, harassment, and so on, while cyber-dependent crimes are crimes like malicious hacking, web defacement, illegal control over IT-systems, malware use, and so on.

Especially these cyber-dependent crimes provide a unique test case for traditional criminological explanations for offending, as these crimes did not exist prior to the rise in the use of IT-systems, the period in which most traditional theories and explanations were developed. Additionally, as will be discussed in more detail later in this chapter, these crimes completely take place in the anonymous and digital context of IT-systems, which could affect the applicability of traditional criminological explanations for offending to cyber-offending. This digital context may change, for example, the situations in which opportunities for committing crime occur, the skills and personality characteristics that are needed to commit these crimes, the perceptions of the consequences of offending, and the interpersonal dynamics between offenders and victims. Even tough cyber-enabled crimes may also heavily rely on a digital context, those crimes could still be committed in physical space. Cyber-enabled crimes vary in the extent to which the digital context is important and almost all traditional crimes could have a digital component. Therefore cyber-enabled crimes are less clearly distinguishable and different from traditional crime than cyber-dependent crime. Consequently, the focus of this dissertation is on cyber-dependent crimes[1] and the question to what extent offenders who commit these crimes differ from traditional offenders.

To illustrate, here are some short descriptions of some of the cyber-dependent crimes that are studied in this dissertation: *Malicious hacking* is a crime in which a person gains illegal access to somebody's IT-system, email account, and so on. This could be done in a technically advanced way, by using vulnerabilities in IT-systems, or just by guessing somebody else's password. *Web defacement* is a crime in which a person changes the content of a website, online profile, and so on., without the owner's permission. *Illegal control over IT-systems* is a crime in which a person has gained that much access to an IT-system that he or she is able to change the processes that take place on the system, without having permission to do so. *Using malware* is a crime in which an offender uses malicious software to manipulate an IT-system. For example, to steal data from that IT-system.

1.3 Traditional explanations for offending

The goal of traditional offender-based criminological research is to explain offending. For traditional crime, there is a very large number of empirical research that tries to find this explanation in a lot of different domains. For this dissertation, I selected four important domains. The overall goal is to empirically compare cyber-offenders with traditional offenders on these domains. In the following sections, these traditional explanations for offending will be briefly discussed. The individual chapters will provide further details.

[1] In the remainder of this dissertation the terms 'cyber-dependent crime' and 'cybercrime' will be used interchangeably to refer to these crimes. The term traditional crime will be used to refer to all other types of crime, including cyber-enabled crimes.

1.3.1 Offending over the life-course

A first important domain in the criminological literature focuses on offending over the life-course. One of the main goals in this area is to examine which life circumstances reduce or increase a person's likelihood of offending. Some important life circumstances that generally reduce this likelihood for an adult are living together with family, being employed and being enrolled in education (for reviews, see Ford & Schroeder, 2010; Kazemian, 2015; Lageson & Uggen, 2013; Skardhamar, Savolainen, Aase, & Lyngstad, 2015; Stouthamer–Loeber, Wei, Loeber, & Masten, 2004). These are life circumstances in which most people have a high stake in conformity as they have more to lose when they commit a crime (e.g., Hirschi, 1969; Sampson & Laub, 1993). Additionally, in these circumstances there is more social control and social support (e.g., Hirschi, 1969; Sampson & Laub, 1993). Lastly, daily activities of people in these circumstances provide less criminal opportunities than the activities of people not living in these circumstances (e.g., Wilcox, Land, & Hunt, 2003). Offending over the life-course will be further discussed in Chapter 2 of this dissertation.

1.3.2 Personal and situational correlates of offending and victimisation

While life-course research generally focuses on changes in one person's life-course that increase or decrease that person's likelihood of offending, there are also between-person differences that explain why some people are more likely to commit crimes than others. Research on these risk factors for offending is an important domain in criminology. Risk factors can be both personal and situational, for example low self-control, substance abuse, and risky life-styles or routine activities. These are, however, also risk factors for victimisation (e.g., Berg & Felson, 2016; Jennings, Piquero, & Reingle, 2012; Rokven, Tolsma, Ruiter, & Kraaykamp, 2016). In addition to a causal relationship between offending and victimisation, these shared risk factors explain the consistent finding that victims are also likely to commit criminal acts, and that offenders also have a relatively high probability of being victimised (e.g., Averdijk, Van Gelder, Eisner, & Ribeaud, 2016; Berg, Stewart, Schreck, & Simons, 2012; Hay & Evans, 2006; Lauritsen & Laub, 2007; Lauritsen, Sampson, & Laub, 1991; Ousey, Wilcox, & Fisher, 2011; Rokven, De Boer, Tolsma, & Ruiter, 2017; Rokven et al., 2016; Schreck, Stewart, & Osgood, 2008). Nevertheless, only a part of the offender population is at risk for victimisation, and not all victims commit crimes. Therefore, in line with recent literature (e.g., Schreck et al., 2008; Van Gelder, Averdijk, Eisner, & Ribeaud, 2015), Chapter 3 of this dissertation will study personal and situational correlates for separate groups of offenders-only, victims-only, and victim-offenders.

1.3.3 Similarity in deviance of social network members

An important and consistently found difference between offenders and non-offenders is that offenders are more likely to have deviant social contacts than non-offenders (e.g., Haynie & Kreager, 2013; Pratt et al., 2009; Warr, 2002; Weerman & Smeenk, 2005; J. T. N. Young & Rees, 2013). This similarity in deviance of social network members has been explained by *influence* and *selection* processes (e.g., Brechwald & Prinstein, 2011; Kandel, 1978). For *influence*, existing deviant social contacts can increase the likelihood of offending by social learning, while existing non-deviant social contacts can reduce the likelihood of offending, as they disapprove criminal behaviour (e.g., Akers, 1998; Hirschi, 1969; Pratt et al., 2009; Sampson & Laub, 1993). *Selection* refers to the preference of non-offenders to associate with non-offenders, while offenders prefer to associate with offenders. This is called homophily (e.g., Hirschi, 1969; Kalmijn, 1998; McPherson, Smith-Lovin, & Cook, 2001). Chapter 4 of this dissertation will focus on this important difference between offenders and non-offenders.

1.3.4 Clustering of offending and motivations for offending

In addition to examining risk factors or life circumstances that influence the likelihood of committing crimes, another way of understanding offending is by examining which crimes often co-occur or are often committed by the same offenders. In other words, to what extent specific types of crime are committed by a specific type of offender. One of the ways of examining differences between these different types of offenders is by asking the question why these offenders commit those types of crime. Traditional criminological theories, for example Routine Activity Theory (Cohen & Felson, 1979), generally just assume the presence of motivated offenders. Their motivation itself is not often specifically investigated. However, it is important to examine those motivations as they may guide us to possible prevention methods. Especially for the type of crime under study, cybercrime, prevention methods are almost non-existent. Therefore, in addition to the established areas of criminological research addressed in Chapters 2, 3 and 4, Chapter 5 of this dissertation will address which types of crime are often committed by the same offender and which motivations the offenders provide for committing those crimes.

1.4 Cyber-offenders versus traditional offenders

Now that the main domains in traditional criminological research that will be addressed in this dissertation have been identified and described, it is important to further consider the possible differences between cyber-offenders and traditional offenders. For each of the domains discussed above, the individual chapter in which that area of criminological research is discussed, will describe in more detail how the context in which cyber-dependent crimes are committed may result in differences between cyber-offenders and traditional offenders in that domain. In the following sections, I will briefly introduce several reasons why cybercrimes and cyber-offenders may differ from traditional crimes and traditional offenders.

First of all, IT-systems are the key component in cyber-dependent crimes, which means that these crimes are committed in a different space and context than traditional crimes. Several authors have argued that for some people it feels like this cyberspace is somehow disconnected from the real world (e.g., Campbell & Kennedy, 2012; Jaishankar, 2009; Suler, 2004). As a result, these people may feel less responsible for their online behaviour and they believe that their online behaviour will not have any real-world offline consequences.

Secondly, in addition to this subjective feeling, apprehension rates for cyber-offending are very low and probably much lower than for traditional crime (e.g., Leukfeldt, Veenstra, & Stol, 2013; Maimon, Alper, Sobesto, & Cukier, 2014; R. Young, Zhang, & Prybutok, 2007). Therefore, objectively, the likelihood of experiencing real-world negative consequences, like punishment, is very low for cyber-offending.

Third, behaviour that takes place in cyberspace is generally less visible and more anonymous (e.g., Campbell & Kennedy, 2012; Jaishankar, 2009; Suler, 2004). This is one of the causes of the low apprehension rates for cybercrime, but also affects the perceived likelihood of negative social reactions from important social relationships. For example, if there are other people physically present, it is almost impossible to commit most traditional crimes, without someone noticing. In contrast, a person could commit a crime in cyberspace, while in the physical space family or colleagues are actually present, but they do not notice what that person is doing on the computer. This could mean that these physically present people cannot exert control over online behaviour to the same extent as they can over offline behaviour.

Fourth, for a cyber-dependent crime to take place, no physical convergence in space and time of offenders and victims is necessary (e.g., Bossler & Holt, 2009; Brady et al., 2016; Holt & Bossler, 2008; Kerstens & Jansen, 2016; Suler, 2004; Yar, 2005a, 2013a). Hence, interactions between victims and offenders are not physical, but take place through an IT-system. This could result in different interpersonal dynamics between offenders and victims when crimes are committed in the digital world compared to interpersonal offenses in the physical world. For example, online interactions can be somewhat asynchronous, i.e. there may be no immediate reaction of the victim after an offender committed a crime. Similarly, an offender will usually not see the emotional reaction of a victim after victimisation (e.g., Goldsmith & Brewer, 2015; Jaishankar, 2009; Suler, 2004; Yar, 2013a).

Fifth, as these crimes take place in a different context than traditional crimes, opportunities for committing these crimes probably also arise in different situations. Therefore, other daily activities may increase or reduce the likelihood of cyber-offending. For example, while the likelihood of committing a traditional crime is higher if a person spends more time outside the home in, for example, nightlife areas (e.g., Bernasco, Ruiter, Bruinsma, Pauwels, & Weerman, 2013; Lauritsen et al., 1991; Sampson & Lauritsen, 1990), the likelihood of committing cybercrime is probably higher if a person spends more time in situations where IT-systems are available, like at home, at work, or at school (e.g., Grabosky & Walkley, 2007; Lu, Jen, Chang, & Chou, 2006; Maimon, Kamerdze, Cukier, & Sobesto, 2013; Nykodym, Taylor, & Vilela, 2005; Randazzo, Keeney, Kowalski, Cappelli, & Moore, 2005; Turgeman-Goldschmidt, 2011; Xu, Hu, & Zhang, 2013).

Sixth, the nature of cyber-dependent offending requires that the offender has at least some IT-skills and knowledge on how to use these skills illegally (e.g., Bossler & Burruss, 2011; Chua & Holt, 2016; Holt, Bossler, & May, 2012; Holt, Burruss, & Bossler, 2010; Holt & Kilger, 2008). These skills are not necessary to commit traditional crimes and acquiring them may require quite some time and effort. In addition, they may be acquired in a different way than skills for traditional offending, for example by reading information on webpages or forums or by watching online videos (e.g., Goldsmith & Brewer, 2015; Holt, 2007, 2009a). The intellectual challenge of breaking an IT-system and acquiring skills in the progress, may even be part of the motivation to commit cybercrimes (Grabosky, 2000, 2001; Grabosky & Walkley, 2007). Lastly, an interesting characteristic of the skills needed to commit cybercrimes, is that these skills can also be used for completely legitimate purposes.

Finally, in relation to the argument that acquiring IT-skills may take time and effort, committing cybercrimes may also require the ability to carefully plan future actions and behaviour (e.g., Bossler & Burruss, 2011; Holt & Kilger, 2008). For cyber-offenders, this ability seems necessary to complete the more sophisticated attacks and cover up one's tracks. For traditional crime, on the other hand, we know that offenders often display a limited ability to think ahead and carefully weigh the costs and benefits of behaviour (e.g., Gottfredson & Hirschi, 1990). Therefore, when comparing cyber-offenders to traditional offenders, cyber-offenders may show, for example, higher self-control. All seven arguments above call into question if the context in which cyber-offenders commit crimes has result in differences between cyber-offenders and traditional offenders.

1.5 Contribution to research on cybercrime

Criminological research on the correlates of cyber-offending can be an important contribution to a field that is dominated by research on technical security prevention techniques. That type of research can help to raise the technical threshold for the offender, but does not address the causes of cybercrime. As argued by Rogers (2011): *'To-date, our strategy has been to focus on technical solutions to the problem, namely, superior firewalls, intrusion detection systems, and stronger passwords. We have ignored the fact that we are dealing with human behaviour and that individuals, not technology, are the true source of the problem.'* (p. 235). Existing empirical criminological work on cyber-offenders has applied traditional theories and explanations for offending to cyber-enabled and cyber-dependent crime (for reviews, see Holt & Bossler, 2014; Weulen Kranenbarg et al., 2017). That work revealed some important correlates of cyber-offending, but it has not taken the possibility into account that some explanations for traditional offending may be less (or more) capable of explaining cyber-offending. Therefore, this dissertation will build on these previous studies, which will provide the background for the comparisons between cyber-offenders and traditional offenders.

In relation to the specific domains addressed in this dissertation, four general conclusions can be drawn from the literature. First, there is no longitudinal research on cyber-offending over the life-course and the extent to which daily activities in and characteristics of the personal and professional life are related to cyber-offending (Holt & Bossler, 2014). Second, just as for traditional crime, there seems to be an overlap in offending and victimisation for cybercrime and this may be caused by overlapping personal and situational risk factors (e.g., Bossler &

Holt, 2009; Kerstens & Jansen, 2016; Morris, 2011; Ngo & Paternoster, 2011; Wolfe, Higgins, & Marcum, 2008). Third, compared to non-offenders, cyber-offenders more often have cyber-deviant people in their social network (e.g., Hollinger, 1993; Holt, Bossler, et al., 2012; Holt et al., 2010; Marcum, Higgins, Ricketts, & Wolfe, 2014; Morris, 2011; Morris & Blackburn, 2009; Rogers, 2001; Skinner & Fream, 1997). Fourth, there is limited empirical work on the extent to which different cyber-dependent crimes are committed by different offenders with motivations that are different from those of traditional offenders. The empirical literature has focused on identifying several motivations for cybercrime (e.g., Bachmann, 2011; Bachmann & Corzine, 2010; Chiesa, Ducci, & Ciappi, 2008a; Denning, 2011; Fotinger & Ziegler, 2004; Gordon & Ma, 2003; Holt, 2007, 2009b; Holt & Kilger, 2012; Jordan & Taylor, 1998; Leukfeldt et al., 2013; National Crime Agency, 2017a, 2017b; Nycyk, 2010; Taylor, 1999; Turgeman-Goldschmidt, 2008; Woo, Kim, & Dominick, 2004; Xu et al., 2013), but the relative importance of these motivations for different types of cyber-dependent offending is still unknown. As these four domains will be discussed in the following chapters, each chapter will provide a more detailed discussion of previous research on cybercrime and traditional crime in that area.

The following chapters will also discuss the limitations of previous empirical work on the specific domains in more detail, but some general limitations that apply to most empirical work on cybercrime should be discussed here. First and foremost, studies have found statistically significant correlates of cyber-offending that are in the same direction as correlates of traditional offending, but empirical comparisons of the strength of these correlates are non-existent. As already discussed, the possibility that explanations for traditional offending may be less (or more) capable of explaining cyber-offending than they are of explaining traditional offending, has not yet been empirically addressed.

Second, previous empirical work has mainly focused on juveniles and has generally used student or school samples and as such cannot be generalised to other populations. Third, these studies mostly focused on crimes that are more prevalent in these samples. Therefore, the focus of previous research on cyber-offending is on cyber-enabled crimes, which are theoretically more similar to traditional crime. In addition, a large body of research has focused on online deviance that is not always criminalised, like watching online pornography, online bullying, and digital piracy. In sum, adults and serious crimes that require more IT-skills are understudied (for reviews, see Holt & Bossler, 2014; Weulen Kranenbarg et al., 2017). This dissertation will address these gaps in the literature by comparing cyber-dependent offending with traditional offending among Dutch adults.

1.6 Data used in this dissertation

The following empirical chapters compare cyber-offenders to traditional offenders on the following domains: offending over the life-course (Chapter 2), personal and situational risk factors for offending and victimisation (Chapter 3), similarity in deviance in the social network (Chapter 4), and motivations related to different offence clusters (Chapter 5). The analyses on these domains are based on two datasets. The first domain will be addressed by using longitudinal population registration data on all adult suspects of cybercrime and traditional crime in the Netherlands during the period of 2000-2012. The other three domains will be addressed by using a dataset that was specifically collected for this dissertation. That dataset contains cross-sectional survey data collected from a high risk sample of both cyber-offenders and traditional offenders. The following sections will briefly describe both datasets.

1.6.1 Longitudinal life-course registration data

For Chapter 2, different longitudinal registration datasets, provided by Statistics Netherlands, have been merged for the complete population of adult Dutch citizens who have at least once been registered in the registration system of the police as a suspect of a cybercrime or a traditional crime in the period 2000-2012. This dataset contains data on 870 unique cybercrime suspects and 1,144,740 unique traditional suspects. For each person, for each year in the period 2000-2012 in which that person lived in the Netherlands and was 18 years or older, the data contain information on household composition, employment, enrolment in education, and cyber-offending and traditional offending. For employment and education, a distinction is made between employment or education in the IT-sector and other types of employment or education. The registration data provide a unique opportunity to longitudinally examine cyber-offending over the life-course, which is new in the field of cybercrime research (Holt & Bossler, 2014).

1.6.2 Cross-sectional survey

Registration data are not specifically collected for research purposes and therefore they cannot be used to answer research questions that require more in-depth measures. Therefore, to examine the other three research domains, I designed a cross-sectional survey to gain in-depth data.

For this cross-sectional data collection, a high risk sample of former suspects of cyber-offences (N = 928) and traditional offences (N = 875) was invited by regular mail to participate in an online survey. The aim was to gain two equally sized groups of cybercrime suspects and traditional suspects. However, response rates were higher among cybercrime suspects, which required inviting a second sample of traditional suspects (N = 781). Eventually two equally sized groups were obtained; 268 cybercrime suspects (28.88% response rate) and 267 (16.12% response rate) traditional suspects completed the online survey[2].

The key parts of the survey are the self-report questions about cyber-offending and traditional offending in the preceding twelve months. Cybercrime questions were based on the Dutch National Cyber Security Centre (2012) list of cyber-dependent crimes and the Computer Crime Index of Rogers (2001). These included: guessing passwords (5.91%), other hacking (4.72%), digital theft (5.31%), damaging data (3.94%), defacing websites or online profiles (5.91%), phishing (2.95%), DoS (Denial of Service) attacks (1.57%), spamming (0.98%), taking control over IT-systems (3.74%), intercepting communication (2.17%), malware use or distribution (2.17%), selling data (1.18%), and selling credentials (0.79%)[3]. Traditional offences were based on Svensson, Weerman, Pauwels, Bruinsma, and Bernasco (2013) and Dutch criminal law. These included: vandalism (3.74%), burglary (1.18%), carrying a weapon (3.94%), using a weapon (0.98%), stealing (5.12%), threats (4.72%), violence (4.53%), selling drugs (2.95%), tax fraud (6.89%), insurance fraud (2.95%), and buying or selling stolen goods (4.33%).

Of all respondents, 69.88% reported that he or she did not commit any of these cybercrimes nor traditional crimes in the preceding twelve months. Furthermore, 10.24% reported to have committed only cybercrime and 12.60% reported to have committed only traditional crime. Lastly, 7.28% reported to have committed both cybercrime and traditional crime. These self-report measures were used in Chapters 3, 4, and 5. A detailed description of the data-collection and the measures that are relevant for the different domains under study can be found in the following chapters. The complete questionnaire (translated into English) can be found in the Appendix at the end of this dissertation.

[2] The total number of respondents who could be used in the analyses in Chapters 3 - 5 differs from these numbers as some participants did not complete the full survey, but did complete all questions necessary to answer some of the research questions in the specific chapters.

[3] These prevalence rates represent the percentage of all respondents who reported to have committed this crime at least once in the preceding twelve months. As there are differences in the total number of respondents who could be used in the analyses in Chapters 3 - 5, the prevalence rates slightly differ between the different chapters.

1.7 Dissertation overview

The following sections will briefly describe the empirical chapters (Chapters 2 - 5). As the chapters are written as individual journal articles some repetition is inevitable. Subsequently, Chapter 6 will provide a general conclusion and discussion of the results of these empirical chapters. This will be followed by a discussion of the overall limitations, future research directions, and practical implications derived from this dissertation.

1.7.1 Longitudinal life-course study (Chapter 2)

The goal of this chapter is to compare cyber-offending with traditional offending over the life-course by examining the extent to which a person's household composition, employment, and enrolment in education influence the odds that he or she commits a cybercrime compared to the extent to which those factors influence the odds that he or she commits a traditional crime. Based on theoretical and empirical literature on traditional crime and a discussion about the unique characteristics of cybercrime, this chapter will argue to what extent these factors are expected to influence cyber-offending to the same extent as traditional offending. These hypotheses will be tested with the longitudinal dataset described above. The longitudinal data structure with repeated measures for each person, enables within-person comparisons of the years in which a person, for example, was employed, compared to the years in which that same person was not employed. This rules out all stable between-individual factors as potential confounds, which allows for drawing strong conclusions.

1.7.2 Correlates of offending, victimisation, and victimisation-offending (Chapter 3)

The goal of this chapter is to examine to what extent there is a cybercrime victim-offender overlap. Subsequently, the goal is to examine which risk factors for offending and victimisation, that have been identified in the literature, are correlated with offending-only, victimisation-only and victimisation-offending. The risk factors include low self-control, online and offline routine activities, and IT-skills. The same questions will be answered for traditional crime, which enables comparing patterns of risk factors related to offending-only, victimisation-only and victimisation-offending between cybercrime and traditional crime.

1.7.3 Similarity in deviance of social network members (Chapter 4)

The goal of this chapter is to compare the strength of the similarity in deviance of social network members between cybercrime and traditional crime. Based on the unique nature of cybercrime it will first be argued that the similarity in deviance is expected to be weaker for cybercrime compared to traditional crime. Subsequently, ego-centred network data, that includes separate observations for the most important social contacts in a person's life, will be used to empirically test this hypothesis. In addition, the data structure allows for testing to what extent similarity in deviance may be the result of similarity in age or gender. Furthermore, it allows for comparing how the correlation between the behaviour of a person and the behaviour of a social contact differs between contacts and to what extent these patterns are similar for cybercrime compared to traditional crime.

1.7.4 Clusters of offences and related motivations (Chapter 5)

The goal of this chapter is to examine to what extent cyber-dependent offenders can be distinguished from traditional offenders, by identifying clusters of cyber-offences and traditional offences in the self-report data. These clusters will show which self-reported crimes are often committed by the same offender and to what extent cyber-dependent offending is a distinct type of crime that does not often co-occur with traditional crime. In addition, it will be explored which motivations the offenders provide for committing these crimes and to what extent a specific cluster distinguishes itself from the other clusters by specific motivations.

Chapter 2

Cyber-offending and traditional offending over the life-course: An empirical comparison*

* This chapter was submitted as: Weulen Kranenbarg, M., Ruiter, S., Van Gelder, J.L., & Bernasco, W. (under review). Cyber-offending and traditional offending over the life-course: An empirical comparison.

Abstract

This paper argues that cybercrime differs from other types of crime in important aspects, which poses challenges to established criminological theory and empirical findings on offending over the life-course. Therefore, this study examines the extent to which life circumstances in the personal and professional life are related to involvement in cybercrime and afterwards empirically compares that to traditional crime. Using longitudinal registration data of all adult suspects of cybercrime (*N* = 870) and traditional crime (*N* = 1,144,740) in the Netherlands during the period of 2000-2012, effects of household composition, employment, and enrolment in education on cyber-offending are compared with those for traditional offending. Fixed effects panel analyses show similar results with respect to people's personal lives. For example, when individuals live together with their partner or their partner and child, they are less likely to commit a cybercrime. For the professional life, on the other hand, some interesting differences were found. There was no strong and statistically significant decreasing effect of employment and enrolment in education on cyber-offending and in this offender population some striking opposite results were found when comparing cyber-offending to traditional offending. This study demonstrated the usefulness of studying cyber-offending over the life-course, but the results also stress the importance of considering possible cybercriminal opportunities provided by otherwise preventive professional life circumstances.

Keywords
cybercrime
cyber-dependent crime
cyber-trespass
life-course
traditional crime
comparison

2.1 Introduction

The prevalence of traditional crime has been declining for several decades now (Tonry, 2014), but cybercrimes show the opposite trend. Police registration data from the Netherlands show that the rate of computer hacking incidents has tripled between 2005 and 2014 (Statistics Netherlands, 2015a). In 2016, malicious hacking (of computers, email accounts, websites or online profiles) was the most often reported crime (4.9%) in a nationwide representative victimisation survey in the Netherlands, followed by vehicle vandalism (4.1%), and bicycle theft (3.8%, Statistics Netherlands, 2017).

Given that cybercrimes are on the increase, and that at least some of their features clearly distinguish them from most traditional crimes, the question is whether established criminological theories and empirical findings on other types of crime are explaining involvement in cybercrime in similar ways. For example, there are several reasons why a person may expect less negative social consequences from committing a cybercrime, compared to committing a traditional crime (e.g., Jaishankar, 2009; Leukfeldt et al., 2013; Maimon et al., 2014; Suler, 2004; R. Young et al., 2007). Significant others may also be less capable of controlling online behaviour compared to offline behaviour. In addition, compared to traditional criminal opportunities, other activities and situations may provide opportunities for committing cybercrimes (e.g., Grabosky & Walkley, 2007; Nykodym et al., 2005; Randazzo et al., 2005; Turgeman-Goldschmidt, 2011). These features make cybercrime a unique test case for existing criminological theories and established empirical findings on traditional crime. The current study looks at cyber-offending over the life-course and examines the extent to which life circumstance in the personal and professional life affect whether an individual commits a cybercrime, capitalizing on unique longitudinal registration data of all suspects of cybercrime and traditional crime in the Netherlands during the period of 2000-2012.

We examine cybercrimes that are '*a direct result of computer technology*' (Furnell, 2002, p. 3). In other words, these are crimes that cannot be committed without the use of IT-systems (Information Technology) and therefore did not exist prior to the advent of those systems. Examples are malicious hacking of computers, email accounts, websites or online profiles; using malware and blocking the access to a website (for example by flooding a website with unwanted traffic; a DDoS (Distributed Denial of Service) attack). Although these crimes have a technical ring to them, it should be noted that some of them actually require little expertise. Hacking an email account, for example, can be done in a technically advanced way, but also by just guessing a password.[1] The cybercrimes in this study could mainly be classified as cyber-dependent or 'cyber-trespass' crimes as defined by McGuire and Dowling (2013) and Wall (2001). These new crimes will be compared to traditional crimes. It is important to note that crimes for which computer technology was used in the commission of the crime, but the type of crime itself already existed before the advent of IT-systems, such as online fraud, online harassment, and child pornography, are also considered traditional crimes in this paper. Those types of crimes could also be committed without the use of IT-systems, whereas the use of IT-systems is a necessary requirement for the cybercrimes in this study. Therefore, these crimes are expected to be most different from traditional crimes.

In this study, we look at cyber-offending over the life-course and examine to what extent life circumstances that normally reduce the likelihood of traditional offending also reduce the likelihood of cyber-offending. These life circumstances are living together with others (for example family), being employed and being enrolled in education. These are life circumstances in which people have a higher stake in conformity as they have more to lose when they commit a crime (e.g., Hirschi, 1969; Sampson & Laub, 1993). Additionally, in these circumstances there is more (informal) social control and social support (e.g., Hirschi, 1969; Sampson & Laub, 1993), both of which have a reducing effect on crime. Also, daily activities of people who live in these circumstances provide less criminal opportunities than the activities of people not living in these circumstances (e.g., Wilcox et al., 2003). These arguments clearly have merit for explaining traditional crime, but the question remains as to whether they can also be successfully applied to explain cybercrime. After summarizing theory and research on traditional offending over the life-course, we will discuss arguments that question the applicability to cybercrime.

2.1.1 Offending over the life-course

As briefly discussed above, criminological literature shows that some life circumstances reduce the likelihood of offending. This is explained with social bonds and social control, as people with strong relationships with others experience both direct and indirect control by these people on their behaviour (e.g., Hirschi, 1969; Sampson & Laub, 1993). Direct control occurs when significant others disapprove or sanction particular behaviour, which is more likely to happen if people have life circumstance in which others are more often around during their daily activities. Indirect control operates through the expectation that sanctioning by others may occur in the future. In order to maintain their strong social bonds, people invest

[1] In Dutch police records, it is unfortunately not possible to systematically distinguish cybercrimes that require advanced technical knowledge and skills from those that do not (Stol et al., 2010; Leukfeldt et al., 2013)

in their relationships, which increases their stake in conformity. Committing crime jeopardizes these investments. Consequently, the more resources people have invested in their relationships, the more they have to lose when they commit a crime.

In addition, life circumstances differ in the criminal opportunities they provide as crimes are often committed during daily activities. Some life circumstances provide more structured daily activities with less criminal opportunities during which there is more supervision of others than in other life circumstances. In these circumstances there is generally also less time to commit a crime than in others (e.g., Wilcox et al., 2003). In this study we focus on life circumstances in both the personal as well as the professional life of adults, as both of these aspects of their live influence their daily activities and the level of social control they experience.

Regarding personal life, social control approaches (e.g., Hirschi, 1969; Sampson & Laub, 1993) assert that people who have invested in a romantic relationship and family life, by having children, have a stronger stake in conformity, which results in having more to lose. Moreover, family life reduces the time spent in criminogenic settings, which also reduces the likelihood of committing crime (Warr, 1998; Wilcox et al., 2003). Recent reviews suggest that there is a strong link between marriage and desistance, but cohabitation, union formation, and parenthood seem to have even stronger effects than marriage (Kazemian, 2015; Skardhamar et al., 2015). We therefore focus on household composition and look at the effects of living together with a romantic partner (both married and unmarried) and living with a child on the likelihood of committing crime.

Regarding professional life, people who have invested in employment commit to that lifestyle, and face the risk of losing their job when they offend. In addition, the presence of superiors and co-workers exerts a degree of control over behaviour (e.g., Hirschi, 1969; Sampson & Laub, 1993). Employment also structures daily activities and leaves less spare time to spend in criminogenic settings (Wilcox et al., 2003) and to commit crime (other than workplace crime). Recent reviews indicate that employment reduces the likelihood of offending (Kazemian, 2015; Lageson & Uggen, 2013).

People's educational careers often extend well into adulthood with increased numbers of people completing a higher education. As a result, they enter the labour market at a later age than in earlier times (Ford & Schroeder, 2010; Payne & Welch, 2015). Therefore, the lives of young adults now often include periods during which they follow education, which makes it important to include enrolment in education in life-course criminological research. After all, if an individual invests in obtaining educational credentials, it increases a person's stake in conformity (Ford & Schroeder, 2010; Payne & Welch, 2015). In the Netherlands, education is only mandatory till the age of 18. Therefore, adults who are still enrolled in education deliberately chose to achieve a certain goal. Similar to employment, enrolment in education makes one spend more time in supervised settings and less time in criminogenic settings (Ford & Schroeder, 2010; Stouthamer–Loeber et al., 2004). Although research on the effect of being enrolled in education on offending among adults is virtually non-existent, Stouthamer–Loeber et al. (2004) found that both employment and enrolment in education were related to desistence.

2.1.2 Cybercrime

Whereas life-course research is an important and well-studied topic for traditional crime, cyber-offending over the life-course and related personal and professional life circumstances have not been studied before. In recent years, research on cybercrime tested the applicability of traditional criminological explanations to cybercrime, mainly focusing on low self-control and social learning (e.g., Holt, Bossler, et al., 2012; Holt et al., 2010; Marcum et al., 2014; Morris & Blackburn, 2009). This previous research also mainly focused on juveniles and traditional forms of delinquency, for which computer technology was used in the commission of the crime, like online piracy and bullying. Adults and crimes that require the use of IT-systems received much less attention (for a review, see Holt & Bossler, 2014).

There are at least five arguments that question the applicability of the aforementioned theory on traditional offending over the life-course to cybercrime and the extent to which the same empirical findings can be expected for cyber-offending over the life-course. First, several authors have argued that people feel as if cyberspace is disconnected from the offline real world (Jaishankar, 2009; Suler, 2004). People may feel that their online behaviour does not carry any real-world offline consequences. Such a disconnect between people's offline and online behaviour may lead them to not feel responsible for their online actions. Second, because the likelihood of apprehension for cybercrime is extremely low (Leukfeldt et al., 2013; Maimon et al., 2014; R. Young et al., 2007), most cyber-offenders never experience any negative social consequences. Consequently, people who do have a stake in conformity in the offline world may still commit cybercrimes, as they may not consider the real-world offline consequences of their online criminal behaviour. Therefore, strong social bonds may not equally affect cybercrime and traditional crime. Third, because online activities tend to be much less conspicuous and more anonymous than most offline behaviour, the impact of direct social control and daily activities on cyber-offending may be limited. The mere presence of significant others may simply not exert the same degree of control over people's online behaviour as it does over their offline behaviour. People may even be able to commit cybercrime irrespective of whether partners, children, colleagues, employers, teachers or fellow students are present in the situation. This could be particularly true if the perpetrator has more IT-knowledge than the others who do not understand what is being done on the computer.

Fourth, because computers are so widely used in most daily activities, life circumstances in which people normally have less traditional criminal opportunities may provide much more opportunities for cybercrime. Those who are employed, for example, use computers more often than those who are not (Statistics Netherlands, 2015b). In addition, having knowledge of and access to a company's IT-system or its data provides employees with opportunities to commit cybercrimes. Several authors have indeed argued that many cybercrimes against businesses are committed by employees (Grabosky & Walkley, 2007; Nykodym et al., 2005; Randazzo et al., 2005). This suggests that cybercrimes are similar to white-collar or employment-enabled crimes in that the job actually offers opportunities for crime instead of a restraint to commit crime (Turgeman-Goldschmidt, 2011). It stands to reason that employment, especially in the IT-sector, increases opportunities and knowledge for cybercrime and that people are therefore more likely to commit a cybercrime when they are employed compared to when they are not.

Fifth, in addition to being an investment in a certain life-style, education can also provide a person with the knowledge to commit cybercrimes, especially IT-related education. Higher educated people indeed have more IT-knowledge than lower educated people (Statistics Netherlands, 2015b), which makes them more capable of committing cybercrimes. In addition to knowledge, schools and universities also provide the students with access to advanced networked computer systems without which it is much harder to commit cybercrime (Lu et al., 2006; Maimon et al., 2013; Xu et al., 2013). For example, by hacking into a university's computer network, an individual can access much greater computer capacity to commit a digital attack than what is possible with only a home computer (Chiesa, Ducci, & Ciappi, 2008b).

All five arguments above call into question whether criminological theory on traditional offending over the life-course is applicable to cybercrime and in case it is, if the effects of life-course factors on cyber-offending are just as strong as they are for traditional crime. A recent Dutch study showed that the age-crime-curves of all suspects of cracking (criminal hacking) in the Netherlands were similar to those of all other Dutch suspects (Ruiter & Bernaards, 2013). However, to date, no studies have assessed what aspects of people's lives affect whether they commit cybercrimes and the extent to which this is similar to or different from the effects found in life-course criminological research on traditional crimes (Holt & Bossler, 2014). This lack of knowledge is largely due to the limited availability of rich longitudinal data on cyber-offending that is required for life-course criminological research. In the present study, we collected precisely this type of data. As this is the first empirical comparison of cyber-offending and traditional offending over the life-course, the most important empirical question that needs to be addressed right now is if in general cyber-offending over the life course is comparable to traditional offending. Overall, previous life-course studies on traditional crime show similar results for different types of traditional crime, therefore the main goal is to compare these general patterns with those patterns for cybercrime. Consequently, and in line with previous studies, we will not distinguish between different types of traditional offending.

2.1.3 The current study

This study looks at cyber-offending over the life-course to examine the extent to which several aspects of the personal and professional life affect whether an individual commits a cybercrime. We combine police data for all suspects of cybercrimes and traditional crimes in the Netherlands for the period of 2000-2012 with population registration data from Statistics Netherlands. These data allow us to estimate fixed effects panel models to obtain the intra-individual effects of changes in household composition, employment, and enrolment in education on cyber-offending and traditional offending. The two models are then compared to examine effect differences. Comparing two models that were both estimated on data from the same source provides the most rigorous test available to date of whether the effects differ between cybercrime and traditional crime.

In line with theory and previous empirical research, we expect that when people live together with a partner or a child they are less likely to commit a traditional crime than when they live alone. For cybercrime, however, we expect that household composition has no effect. In line with previous research, we expect that employment and enrolment in education will decrease the odds of committing traditional crime. However, for cybercrime we predict the opposite; namely that employment and enrolment education *increase* the odds of committing cybercrime, especially if employed in the IT-sector or enrolled in IT-related education.

2.2 Data and methods

2.2.1 Data

This study uses panel data from the years 2000-2012 (with the exception of 2010[2]) on the entire population of adult suspects of crime in the Netherlands. The dataset contains information for each year on all variables described below for each person who was a suspect of a crime at least once during the period of 2000-2012, aged 18 or older and registered as a resident of a Dutch municipality (registration is mandatory for all residents in the Netherlands). Some people emigrated or passed away during the study period. For these individuals only the years in which they lived in the Netherlands are included in the analysis.

For cyber-offending, the dataset consisted of 870 unique persons[3] with 8,752 person-years of data, which means an average of 10.06 (*SD* = 2.90) years per person in the dataset. For traditional crimes, the dataset contains 1,144,740 unique persons with 11,840,665 person-years of data, implying an average of 10.34 (*SD* = 2.79) years per person. 470 people were included in both datasets as they were at least once suspected of a cybercrime and at least once of a traditional crime. The Appendix provides more detail about the construction of the dataset.

Those who committed cybercrimes were on average younger (*Myears* = 33.35, *SD* = 10.77) than those who committed traditional crimes (*Myears* = 37.97, *SD* = 13.70) across all person-years. In both groups, approximately 80 percent were male. The group of cybercrime suspects consisted of slightly more people of native Dutch origin (71%) than the group of traditional suspects (66%), but the other ethnic backgrounds were similarly distributed across both groups.

[2] On October 1st 2010, the Dutch criminal law on malicious hacking changed. Until that day, unauthorised access into an IT-system was criminalised under criminal law 138a. From that day, squatting a house was criminalised by 138a. Because the data are only available at the annual level, it is impossible to distinguish the people who were a suspect of malicious hacking from those suspected of squatting in 2010. We therefore excluded the year 2010 from the analysis as presented here. However, as a robustness check we also estimated our models 10 times using all data from 2000-2012 while randomly assigning a weighted proportion of the 138a suspects to the group of people who committed a cybercrime in 2010 and subsequently applying Rubin's formulae (1987) (1987) to calculate the overall effect sizes and standard errors. The results were almost identical to those presented here and can be requested from the first author.

[3] Statistics Netherlands requires rounding of absolute numbers about suspects of crime to multiples of 10 and percentages to whole numbers.

2.2.2 Dependent variables

Data on whether an individual was a suspect of a crime in a particular year were derived from the longitudinal registration system of the Dutch police, which includes every person for whom a Dutch police department filed a report. Special investigation units that are not part of the police, such as the tax and customs authorities, do not register their suspects in this system. For a more detailed description, see the Appendix.

Cyber-offending was constructed as a dichotomous variable that indicates whether or not a person was a suspect of at least one cybercrime in a given year. As discussed in the introduction, all cybercrimes in this sample are crimes that could not have been committed without using an IT-system. The most common cybercrimes in this sample were different forms of system trespassing, ranging from password guessing to advanced hacks.

Traditional offending was also defined as a dichotomous variable that indicates whether or not a person was a suspect of at least one traditional crime in a given year. The most common traditional crimes in the sample were property crimes (27.89%), violence (21.03%), serious traffic crimes like dangerous driving while intoxicated (19.33%), and public order crimes like vandalism (14.99%).

2.2.3 Independent variables

In order to ensure that the personal and professional life circumstances (independent variables) described below precede the involvement in cybercrime and traditional crime (dependent variables), all independent variables (unless stated otherwise) reflect a person's situation on January 1st of a particular year. For more information on the exact source and construction of the independent variables, see the Appendix.

For *household composition*, we distinguish between individuals who live alone, individuals who live with a romantic partner (married or unmarried), individuals who live with a partner and one or more children, individuals who live with one or more children but without a partner, and individuals who live in a household composition different from the above. The latter category contains those who lived with their parents (73.60%), lived with others (11.88%), were institutionalised (6.74%), and unknown household composition (7.78%)[4]. In the analyses, 'living alone' is used as the reference category.

[4] 99.86 percent of the unknown category immigrated to the Netherlands during the year and therefore the household composition on January 1st was unknown. We also estimated models with dummy variables for all household compositions separately, but all other estimates in the models were largely the same. The additional models can be requested from the first author.

Employment is measured using three dummy variables that indicate whether a person was not employed, employed outside the IT-sector, or employed in the IT-sector. Employment includes self-employment. For self-employment there was no information available about a person's situation on January 1st, therefore for self-employment the employment dummy variable reflects whether a person was self-employed at any time during a given year, instead of on January 1st of that year. In the analyses, 'not employed' is the reference category.

Education is also measured using three dummy variables. Because the educational year starts in September, people are considered to be enrolled in education on January 1st if they started the education in September the year before. We distinguish those who are not enrolled in education from those who are enrolled in non-IT education and those who are enrolled in IT-related education. In the analyses, 'not in education' is the reference category.

In longitudinal analyses, it is essential to include an *exposure* measure that captures the degree to which an individual was actually at risk of committing a crime that could have been recorded in the police data. We used the number of days in a year that an individual lived in the Netherlands and had not passed away, divided by 365 to obtain a variable that could range from zero to one. This variable does not reflect the situation on January 1st but exposure throughout the entire year. Although incarceration data were not available, we included as a predictor variable the number of days (also divided by 365) a person had lived *institutionalised*, because this category includes (but is not restricted to) people who were incarcerated.

2.2.4 Analytical strategy

Taking advantage of the panel structure of the data, in which repeated measures of the same person are available, the hypotheses were tested with fixed effects regression models. These models only consider intra-individual but not inter-individual differences. Therefore, they rule out all stable between-individual factors as potential confounds and thus allow for relatively strong conclusions (Brüderl & Ludwig, 2014)[5]. Because the outcome variables are dichotomous (whether or not to be a suspect of crime in a particular year), the fixed effects logit model is most appropriate. The parameter estimates will be presented as odds ratios. The odds

[5] A small disadvantage of these models is that relying on intra-individual differences implies that some intra-individual variation must exist in the dependent variable. They therefore require that every person in the analysis had at least one year of offending and at least one year of non-offending. For this reason, the 9,180 people of whom only information on a single year was known, and the 7,460 people who were a suspect of crime in every year during the study period, were excluded from the analysis.

ratio for a specific independent variable indicates by which factor the odds of being a suspect change as a function of a one-unit increase in the independent variable.

The standard fixed effects model only controls for time-stable between-person heterogeneity. However, whether people become suspects of crime also varies over time due to factors such as the capacity and prioritisation of the police. This is especially the case for cybercrime. The availability of IT-systems in general and the knowledge and specialisation of the police increased during the study period, which is reflected by a sharp increase in the number of suspects of cybercrime during those years (Leukfeldt et al., 2013). Without taking these period effects into account, our results could be biased. We therefore estimate a so-called two-way error component model which controls for age and period effects by including year dummy variables (Baltagi, 2005). We use the seemingly unrelated estimation procedure as developed for Stata (Weesie, 1999) for testing whether the parameter estimates differ between the cybercrime and the traditional crime models. This allows for testing between models based on the same, different, or partially overlapping datasets with different sample sizes.

2.3 Results

2.3.1 Descriptive and bivariate analyses

In this section, we first discuss descriptive statistics and bivariate relationships of the variables under study, followed by a comparison of the fixed effects logit models for cyber-offending and traditional offending. The first three columns of Table 2.1 show the population averages across all person-years in the Dutch adult population, the population of cybercrime suspects, and the population of traditional suspects respectively. As can be seen in the table, cybercrime suspects and traditional suspects more often live on their own and more often live in a single parent household than the general population. The last two columns of Table 2.1 show the percentage of years in which people commit cybercrimes and traditional crimes, conditional on the row category. These bivariate relationships show that cybercrimes were mostly committed when people lived alone or in a single parent household and less often when they lived with a partner or a partner and a child. For traditional crimes, these bivariate results are quite similar, although cyber-offending is more likely than traditional offending when people live in single-parent households.

Regarding employment, the first three columns of Table 2.1 indicate that both offender populations are more often employed than the average Dutch population. However, the last two columns show that most cybercrimes and traditional crimes are committed in the years in which people are actually not employed. Cybercrime suspects are also much more often employed in the IT-sector and cybercrimes are more often committed in the years in which people are employed in the IT-sector than in years in which they have some other type of employment. Traditional crimes on the other hand are less often committed in years of employment in the IT-sector.

Table 2.1.
Life-course variables prevalence rates among Dutch adult population and offender population and their bivariate relationships with cybercrime and traditional crime

	Prevalence rate (%)			Bivariate relationship[b] (%)	
Variable	**Dutch population[a]**	**Cyber-offender population**	**Traditional offender population**	**Cybercrime group**	**Traditional crime group**
Household composition					
Alone	19.07	26.97	25.84	11.40	17.92
With partner	32.50	16.84	19.52	8.55	12.00
With partner & child	32.24	26.71	27.42	7.83	12.25
With child	3.42	4.00	5.30	13.71	14.54
Other	12.76	25.48	21.92	11.52	21.80
Employment					
Not employed	42.56	34.26	38.63	11.57	19.07
Employed non-IT	56.43	59.95	60.59	9.22	13.92
Employed IT	1.01	5.79	0.78	10.26	11.15
Education					
Not in education	96.02	94.46	96.41	9.80	15.74
In non-IT education	3.85	4.44	3.47	14.65	19.78
In IT-education	0.13	1.10	0.12	16.67	17.82
Total (%)	100.00	100.00	100.00	10.09	15.88
N (person-years)	7,727,398[c]	8,752[d]	11,840,665[e]	883	1,880,696

a: Based on a random sample of 5% of the Dutch population.
b: The percentage of years in which cybercrimes/traditional crimes are committed, conditional on the row category.
c: unique persons: 791,046
d: unique persons: 870*
e: unique persons: 1,144,740*
* absolute numbers of unique suspects are rounded to multiples of ten.

Cyber-offenders and traditional offenders also differ with respect to enrolment in education. Cyber-offenders are more often enrolled in education than the general population, whereas traditional offenders are less often enrolled in education. Enrolment in IT-education is also much more common among cyber-offenders. The last two columns show that cybercrimes are more often committed when a person is enrolled in education, especially when enrolled in IT-education. Traditional crimes are also more often committed when people are enrolled in education, but less often when enrolled in IT-education.

2.3.2 Fixed effects logit models

The descriptive statistics and bivariate relationships presented above already suggest that the effects of household composition are relatively similar for cyber-offending and traditional offending, whereas the effects of employment and enrolment in education, especially IT-related employment and education, differ between the two groups. However, some of the bivariate differences may be due to aging or to changes in some of the other variables that occur at the same time. We will therefore discuss the results of the fixed effects logit models in which all variables are included simultaneously and in which we also control for age and period effects by including a dummy variable for each year. Multicollinearity was not an issue in these models, as no VIF was over 1.55. We do not limit the discussion of our results to statistically significant effects, because non-significant effects and differences may still reflect important differences within these populations.

Table 2.2 shows the estimated odds ratios of the fixed effects logit models for cybercrime and traditional crime respectively. The odds ratios represent the change in the odds an individual commits a crime[6] in a given year when the independent variable increase one unit, typically from 0 to 1, holding everything else constant. Odds ratios above one reflect positive effects and odds ratios below one represents negative effects. For example, Table 2.2 shows an odds ratio of .69 for living with a partner. This represents a negative effect, and means that the odds an individual commits a cybercrime decrease by 31 percent ((1 - .69)*100) when a person changes from living alone to living with a partner ($p < .05$).

[6] It should be noted that the outcome variables actually represent being registered as a cybercrime suspect or traditional suspect in the police registration data. It is unknown to what extent a person also committed crimes in the years he or she was not registered as an offender.

Table 2.2.

Results of fixed effects models for committing cybercrime and traditional crime

	Cybercrime		Traditional crime		Model comparison
Characteristic	**OR**	**SE**	**OR**	**SE**	**χ^2(df)**
Household composition					11.66(4)*
Alone	-	-	-	-	-
With partner	.69*	.11	.79***	.00	.75(1)
With partner & child	.54***	.09	.81***	.00	5.79(1)*
With child	1.81*	.53	1.07***	.01	2.83(1)†
Other	.84	.12	.98***	.00	1.04(1)
Employment					1.40(2)
Not employed	-	-	-	-	-
Employed non-IT	.90	.10	.93***	.00	.06(1)
Employed IT	1.14	.28	.89***	.01	1.02(1)
Education					.74(2)
Not in education	-	-	-	-	-
In non-IT education	1.10	.24	.92***	.01	.63(1)
In IT-education	1.06	.41	.88***	.03	.23(1)
Exposure days	1.12	.40	1.39***	.01	.38(1)
Days institutionalised	.52	.23	.69***	.01	.34(1)
N (person-years)		8,752		11,840,665	
Unique persons[a]		870		1,144,740	
All characteristics combined (χ^2(df))					227.74(21)***

† p<.10; * p<.05; ** p<.01; *** p<.001 (two-tailed)

a: absolute numbers of unique suspects are rounded to multiples of ten.

Note: Separate year dummy variables were included in the models to control for age and period effects, but these are not displayed in the table.

OR = odds ratio

SE = standard error

df = degrees of freedom

Household composition

In contrast to our expectations, the household composition effects for cybercrime are in the same direction and even stronger than those for traditional crime. The joint test of effect differences shows a statistically significant difference in household composition effects for cyber-offending and traditional offending ($\chi(df)^2$ = 11.66(4); p < .05). For example, while living with a partner and a child decreases the odds a person commits a cybercrime by 46 percent (p < .001), this household composition decreases the odds of committing a traditional crime by only 19 percent ($p <$ .001). The last column of Table 2.2 shows that these effects also differ statistically significantly ($\chi(df)^2$ = 5.79(1); p < .05). Similarly, living with a partner reduces the odds a person commits a cybercrime by 31 percent (p < .05), whereas the odds are only reduced by 21 percent (p < .001) for traditional crime. In general, the results show that the households with more social control have stronger decreasing effects on cybercrime than on traditional crime. The results for single-parent household are, however, unexpected. If an individual is living as a single-parent that person is considerably more likely to commit a cybercrime (OR: 1.81) and somewhat more likely to commit a traditional crime (OR: 1.07), compared to when that person is living alone. Although the effect on cybercrime appears to be much stronger, the difference in effects is only marginally significant ($\chi(df)^2$ = 2.83(1); p<.10).

Employment

Both models show similar effects for non-IT employment, although the results for cybercrime are not statistically significant. If an individual has a job, this reduces the odds that person commits a cybercrime and traditional crime by 10 and 7 percent (p<.001) respectively. For IT-employment, however, we find opposite results. It increases the odds of committing a cybercrime by 14 percent, whereas it decreases the odds of committing a traditional crime by 11 percent (p<0.001). This 11 percent decreasing effect of IT-employment for traditional crime is statistically significantly stronger than the 7 percent decreasing effect of general employment for traditional crime ($\chi(df)^2$ = 6.36(1); p<.05; results not shown), while IT-employment increases cyber-offending (not statistically significant).

Education

For enrolment in education, we find opposite effects for cyber-offending and traditional offending. Being enrolled in education increases the odds of committing a cybercrime. Although not statistically significant, the effect of enrolment in non-IT education (OR: 1.10) is somewhat stronger ($\chi(df)^2$ = .01(1); p = .91; results not shown) than the effect of IT-education (OR: 1.06). Both enrolment in IT-education (OR: .88) and non-IT education (OR: .92) reduces the odds of committing a traditional crime. Although neither the estimates for cybercrime nor the results of the joint tests of effect differences are statistically significant, the opposite direction of the effect of enrolment in education is a fascinating finding in this population.

2.4 Conclusion and discussion

Because cybercrimes possess several unique features not found in most conventional types of crime, they may pose a challenge to existing criminological theories and established empirical findings. We examined this claim by investigating cyber-offending over the life-course. We employed fixed effects logit models on longitudinal population registration data of all adult suspects of cybercrime and traditional crime in the Netherlands from the period of 2000-2012 to test whether the effects of household composition, employment, and enrolment in education on the likelihood of committing cybercrime differed from those for traditional crime. We argued that some otherwise preventive life circumstances would not prevent people from committing cybercrime, because they may feel as if their behaviour in cyberspace has no real-world consequences and significant others are less capable of controlling online behaviour. We also suggested that those life circumstances may actually provide more opportunities to commit cybercrime than other life circumstances.

Contrary to our expectations, we found that the effects of household composition on cybercrime were in the same direction and even stronger than those for traditional crime. When individuals live together with others they are less likely to commit a cybercrime than when they live on their own. Although exerting social control on people's online behaviour is difficult, these results suggest that family members do have some inhibiting effect which reduces the likelihood of cyber-offending. It is possible that the assumption that spending more time at home with a family would expose people to more opportunities for committing cybercrime is misguided, or that the positive effect of those opportunities is offset by the direct and indirect social control exerted by family members. However, the results also showed that individuals living as single parents are much more likely to commit a cybercrime and only somewhat more likely to commit a traditional crime than when they live alone. Future research could further investigate whether this positive effect occurs because single parents are indeed more exposed to opportunities for cybercrime or because they experience limited social control over their online behaviour.

In line with our expectations, we did not find a strong and statistically significant protective effect of employment and enrolment in education on cyber-offending. In the complete offender population in this study, we even found that employment in the IT-sector and enrolment in education increase the odds an individual commits a cybercrime, while they decrease the odds of committing a traditional crime. However, non-IT employment decreases the odds of both cyber-offending and traditional offending. This suggests that stronger social control and professional life circumstances can prevent an individual from committing a cybercrime in general, but some otherwise non-criminogenic settings such as IT-employment and education can provide opportunities to commit cybercrimes, while the social control to prevent these crimes from happening may not be strong enough in these settings. It should be noted however that the latter results were not statistically significant for cybercrime and therefore only represent effects within this population. Future research could therefore examine if results can be replicated in different samples and different time periods. Future work could also attempt to identify the micro-situations in people's daily lives that expose them to opportunities for committing cybercrime.

This study was also prone to a number of limitations that require discussion. Fixed effects panel models are relatively rigorous because they eliminate all stable (observed or unobserved) between-individual variability as potential confounds and therefore better justify causal claims than most other methods for analysing observational panel data. Fixed effects panels, however, cannot account for unmeasured time-varying factors that may have influenced the likelihood of offending. For example, people become involved in romantic relationships without living together or change their daily activities for reasons unrelated to family life, employment, or education. We have no way of knowing whether such changes in people's lives confound our results. However, we did include several indicators for both the personal and professional life of people that were identified to be most important in life-course criminology. Instead of studying marriage and parenthood, we analysed the effect of a person's household composition, which better captures the actual situation a person lives in. We took care to ensure that the causal order of the variables was correct by using the situation on January 1st to construct most of our independent variables. However, because the crime data were only available at the annual level we cannot be sure the situation still existed at the time of the offence.

Another point for discussion is that this study relied on police suspect data as self-report data or conviction data were unavailable. This means that it is unknown to what extent a person also committed crimes in the years he or she was not registered as a suspect. In addition, whether the suspects were actually guilty of committing the crimes of which they were a suspect is unclear. However, it is known that about 90 percent of all suspects are eventually convicted in a criminal court or their cases get settled out-of-court by the public prosecutor. It is also difficult if not impossible to generalise our results to the cyber-offender population, because so many cyber-offenders operate from other countries and many do not come into contact with the police. It has, for example, been argued that the most technically skilled cyber-offenders operate from other countries (European Cybercrime Center, 2014). In addition, in the Dutch police records as used in this study, cybercrimes that require advanced technical knowledge cannot be distinguished from those that do not (Leukfeldt et al., 2013; Stol, Leukfeldt, & Domenie, 2010). This lack of specificity in the outcome variable means that cybercrimes that require advanced technical knowledge are combined with cases in which the suspect, for example, only guessed another individual's password to break into a computer system. Should such distinction have been possible, it would have been interesting to test whether enrolment in IT-education and IT-employment more strongly affect technically complex cybercrimes. Future research could further investigate the knowledge and opportunities needed for more technically complex cybercrimes and the extent to which these are related to specific life circumstances.

The advantage of using police registration data is that they provide information on all suspects of crime instead of a sample. Even parameter estimates that are not statistically significant still reflect differences among these suspect populations. At the moment, this is the best available data that is suited to compare people who were a suspect of a cybercrime with those who were a suspect of a traditional crime, because the data for both groups originated from the same source. It should be noted, however, that it is impossible to know to what extent the selection process that results in being registered as a suspect in the police registration data, may differ between cybercrime suspects and traditional suspects. If there are structural differences in this selection process, this could potentially affect the comparability of the two suspect populations used in this study. Nevertheless, these two populations are more comparable than two populations that would originate from a different source.

In our analyses we compared a specific group of cybercrime suspects with a diverse group of traditional suspects. As this is the first study that compares cyber-offending and traditional offending over the life-course, this general comparison of general patterns in the life-course addressed the most important research question at this moment. Future research may disaggregate the dependent variable and test whether stronger similarities are found if cyber-offending is compared with specific types of traditional offending, for example employment-enabled crimes. In such studies, the effect of IT-employment could then be compared to the effect of specific types of employment that enable white-collar crimes. To illustrate, future studies could address the question whether the effect of following education in finance or employment in the finance sector on committing fraud is similar to the effect of following IT-education or IT-employment on cybercrime.

Compared to the large and strong body of traditional life-course research our research based on registration data of course has its limitations. Nevertheless, it provides unique insights in the possible differences between cyber-offending and traditional offending over the life-course. Using fixed effects panel models on a group of cyber-offenders and a comparison group of traditional offenders, we generated results that are new to cybercrime and life-course research. To further advance the field, new life-course research is needed to replicate these findings in different populations. Longitudinal self-report studies are advised to start including questions on cyber-offending, because that could further enhance our knowledge of non-registered life circumstances on (non-registered) cyber-offending. Such studies could also include detailed questions on the strengths of social bonds and people's actual daily activities, because these cannot be measured in studies that use registration data. For example, these studies could see if the effects of employment are the result of changes in social bonds and social control, changes in daily activities and opportunities, changes in financial situation, etcetera. Furthermore, more knowledge is needed about the way IT-employment and education could provide opportunities for cybercrime and how this can be prevented.

With this paper, we demonstrated the usefulness of studying cyber-offending over the life-course. We tested whether life-course criminological findings for traditional crimes also apply to cybercrime. The comparison shows similar results with respect to people's personal lives, but the results also stress the importance of considering the possible cybercriminal opportunities provided by otherwise preventive life circumstances, in particular IT-related employment and enrolment in education.

2.5 Appendix: dataset composition

The dataset was constructed by using several individual-level datasets provided by Statistics Netherlands. To facilitate replication, a list of names in Dutch of all the datasets used is provided at the end of this Appendix. The individual-level datasets were anonymised and included a non-informative unique personal identification number. We combined the data using these unique identifiers. Below we describe each dataset in more detail.

Dependent variables

Data on crime suspects were derived from the police registration system *Herkenningsdienstsysteem*, a longitudinal registration system of the Dutch police that includes every person for whom a police department filed a report. Special investigation units that are not part of the police, such as tax- and customs authorities, do not register their suspects in this system. This means that some economic crimes, environmental offences, or benefit frauds are not registered in this system. For a more detailed description, see Bernasco (2010a).

In the Netherlands, the cybercrimes that have emerged as '*a direct result of computer technology*' (Furnell, 2002, p. 3) are criminalised under specific articles of Dutch criminal law (National Cyber Security Centre, 2012), which were used to determine whether a crime was a cybercrime or a traditional crime. The articles of law are: Sr138ab.1; Sr138ab.2; Sr138ab.3; Sr138b; Sr139d; Sr139e; Sr161sexies; Sr161septies; Sr350a.1; Sr350a.2; Sr350a.3; Sr350b.1; Sr350b.2; and until 2010: SR138a.1; SR138a.2; SR138a.3

Independent variables

Several individual-level datasets were based on the Dutch registration system of municipalities, the *Basisregistratie personen* (Dutch acronym: BRP). For more information about this nationwide system, see Blokland and Nieuwbeerta (2005). For our analyses, we extracted date of birth, gender, ethnicity, days living in the Netherlands, days alive and household composition from the Statistics Netherlands' individual-level datasets on demographics, international immigration, deceased persons and households of all people who are registered in BRP. The dataset on households is almost completely derived from the BRP. Only five percent of the information on household compositions is based on registers of taxes, income support, governmental funding on healthcare and rental allowance. Another five percent is imputed by using information from the Labour Force Survey (in Dutch: Enquête Beroepsbevolking; for more information, see Statistics Netherlands, 2014a).

Employment and self-employment were derived from individual-level datasets on job characteristics, yearly job summary statistics, business characteristics, and people who had taxable income out of their own business. These datasets are a combination of data from registration of income taxes, administration of employee insurance, the Survey on Employment and Wages, the Earnings Production System, and the registration system of self-employment. Employment in the IT-sector was constructed using the SBI classification system, which is based on the NACE of the European Union and the ISIC of the United Nations. For the years 2000-2005 we used the SBI 1993 classification (classification numbers 7210, 7221, 7222, 7230, 7260) and for the years 2006-2016 we used the SBI 2008 classification (classification numbers 6201, 6202, 6203, 6209) to identify IT-employment. These classification numbers include the following sectors: developing and producing software, hardware consultancy, software consultancy, computer facilities management, software implementation, etcetera. For more information, see Statistics Netherlands (2014b).

Whether or not an individual was enrolled in education was derived from the individual-level dataset on highest education. We used changes in completed educational level and attended educational level to derive the start and end dates of a specific education. A person was considered to be enrolled in education between the years in which he or she started and ended the education. In addition, if a person started an education that in general takes more years than the remaining years in the dataset, the person was considered to be enrolled in education from the start until the last year included in the dataset. This could have caused a slight overestimation of the number of people enrolled in education, as it was not possible to exclude school drop-outs. In a similar way, people who completed an education that generally takes more years than they were in the dataset were also considered to be enrolled in education until the moment they ended that education. As this variable is constructed by using changes within the period of 2000-2012 in an individual’s formally registered educational level and qualifications, it does not reflect non-registered education and it may slightly underestimate the number of people enrolled in education, because it cannot detect people who are enrolled in education but do not change in their educational level during the period of 2000-2012. This dataset is a combination of data from registers for government-funded high schools, secondary vocational education and adult education, the Central Register of Higher Education Programs, the exam register for secondary education, registration of governmental student financing, the governmental employee insurance agency and the Labour Force Survey. IT-education was constructed using the International Standard Classification of Education ISCED 1997 (UNESCO, 1997). For identifying IT-education, we used the category ‘computing’ (field of education number 48), which are computer sciences or education like: system design, computer programming, data processing, networks, operating systems, and software development.

Combining all these separate datasets resulted in a person-year dataset. Each observation in the dataset contained information on all variables for one specific year for one individual. The used micro datasets are named:

- BAANKENMERKENBUS
- BEBUS
- GBAHUISHOUDENSBUS
- GBAMIGRATIEBUS
- GBAOVERLIJDENTAB
- GBAPERSOONTAB
- HKS (land_delikt & land_ant_del)
- HOOGSTEOPLTAB
- ZELFSTANDIGENTAB

For more information about the used datasets, see http://www.cbs.nl/en-GB/menu/informatie/beleid/zelf-onderzoeken/default.htm

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, 2011; 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[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

[1] 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 (*Myears* = 38.49 compared to *Myears* = 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: 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 3.1.

Table 3.1.
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

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 (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).

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[2]. 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[3].

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 * 245) / (37 * 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 * 225) / (31 * 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

Cybercrime victimisation					Traditional victimisation				
	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 victimisation	1.52	0.96	1.89	1.20*	Types of victimisation	1.77	1.24	2.52	1.67***

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

Table 3.3.

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	Use weapon	0	0.00	2	3.17
DoS	1	2.70	4	9.09	Sell 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	Types of offending	1.61	0.95	2.05	1.60

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

	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	χ^2(df)	χ^2(df)	χ^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)	3.30(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)

Table 3.4.

Continued

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)
N		37		133		44		31		140		63			
Combined comparison													33.52(20)*	47.82(20)***	44.29(20)**

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

1. LR $\chi^2(60)$ = 127.73; Reference group is: neither victim nor offender cybercrime (N = 245)

2. LR $\chi^2(60)$ = 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. 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.

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.

Chapter 4

Do cyber-birds flock together? Comparing similarity in deviance among social network members of cyber-offenders and traditional offenders*

[*] This chapter was submitted as: Weulen Kranenbarg, M., Ruiter, S., & Van Gelder, J.L. (under review). Do cyber-birds flock together? Comparing similarity in deviance among social network members of cyber-offenders and traditional offenders.

Abstract

Cyber-dependent crime takes place in the anonymous digital context of IT-systems. Because of this context, we argue that the relation between deviance of an individual and deviance of social network members is weaker for cybercrime compared to traditional crime. We test this by comparing ego-centred networks of suspects of cybercrime and traditional crime in The Netherlands (*N*=346). Results show that similarity in deviance is statistically significantly weaker for cybercrime than it is for traditional crime. Findings also show both similarities and differences between the crimes, in the way similarity in deviance differs between social network members. For research and prevention strategies our findings suggest that traditional crime predictors, like deviance of social contacts, cannot always be assumed to be equally important for cybercrime.

Keywords
cyber-dependent crime
cybercrime
ego-centred social networks
comparison traditional crime
similarity in deviance

4.1 Introduction

The expansion of the internet has created many new opportunities, and among them opportunities for cybercrime. For some traditional forms of crime like fraud, offenders now use IT-systems. Such crimes are called cyber-enabled. Even more striking, is the emergence of complete new forms of crime, cyber-dependent crime, like illegal hacking, defacing, taking control over IT-systems, and so on (e.g., Grabosky, 2017; Tcherni et al., 2016). These crimes cannot be committed without the use of IT-systems and therefore they completely take place in an anonymous digital context, where there are no physical social interactions (e.g., Jaishankar, 2009; Suler, 2004; Yar, 2013a) and offending requires IT-skills and knowledge on how to use those skills illegally (Holt et al., 2010). These conditions challenge the extent to which criminological theories and established research findings on traditional crime also apply to cyber-dependent crime. Nevertheless, most cybercrime research to date has focused on cyber-enabled deviant behaviour like bullying, harassment, fraud, sexual deviance, or piracy (for a review, see Holt & Bossler, 2014), rather than cyber-dependent crime.

One of the most established empirical findings for traditional crime is that there is a strong relationship between the criminal behaviour and the attitudes of a person and the criminal behaviour and attitudes of that person's social network (e.g., Haynie & Kreager, 2013; Pratt et al., 2009; Warr, 2002; Weerman & Smeenk, 2005; J. T. N. Young & Rees, 2013). This relationship has been explained by influence and selection processes. Research on cyber-offenders has shown that compared to non-offenders, offenders also more often have cyber-deviant social contacts (e.g., Hollinger, 1993; Holt, Bossler, et al., 2012; Holt et al., 2010; Marcum et al., 2014; Morris, 2011; Morris & Blackburn, 2009; Rogers, 2001; Skinner & Fream, 1997). Nevertheless, it is unclear if the digital context has an impact on processes of selection and influence. Is cyber-dependent crime different from traditional crime in the extent to which there is similarity in deviance among social network members? To date, this question remains unanswered.

In this paper we will empirically compare cyber-dependent offending, which we will call cyber-offending, with traditional offending, which are all other types of offending. We will use ego-centred network data on core discussion networks from an online survey among adult cybercrime and traditional former suspects in The Netherlands. We will compare the relationship between cyber-deviant network members and cyber-offending with the relationship between traditional deviant network members and traditional offending. In addition, we will explore if cybercrime is comparable to traditional crime in the way the correlation between the behaviour of a person and the behaviour of social contacts differs between contacts. Specifically, whether the correlation is stronger for contacts who are contacted daily, and who are identical in age and gender.

4.1.1 Similarity in social networks

Similarity in behaviour in social networks has been explained by *influence* and *selection* processes (e.g., Brechwald & Prinstein, 2011; Kandel, 1978). For deviant behaviour the *influence* of existing deviant social contacts can increase the likelihood of offending by social learning. Existing non-deviant social contacts can reduce the likelihood of offending, as they disapprove criminal behaviour (e.g., Akers, 1998; Hirschi, 1969; Pratt et al., 2009; Sampson & Laub, 1993). *Selection* refers to the preference of non-offenders to associate with non-offenders, while offenders prefer to associate with offenders, this is called homophily (e.g., Hirschi, 1969; Kalmijn, 1998; McPherson et al., 2001). For offenders, deviant contacts will be less likely to disapprove criminal behaviour, which reduces the risk of negative social reactions and contacts reporting crimes to the police (e.g., Flashman & Gambetta, 2014). Deviant contacts can also provide criminal sources of information, resources, and accomplices. In addition, selection can be the result of daily activities that increase the chance of associating with others who show similar behaviour. Lastly, social networks become even more homogeneous because current deviant contacts influence who will be a new social contact, while differences in behaviour could result in ending relationships (e.g., Hirschi, 1969; Kalmijn, 1998; McPherson et al., 2001; Rokven et al., 2016).

4.1.2 Empirical evidence for similarity in traditional and cyber-deviant behaviour

For traditional crime, numerous studies have found evidence for similarity in deviant behaviour in social networks, and both selection and influence seem to partly explain it (for reviews, see Haynie & Kreager, 2013; Pratt et al., 2009; Warr, 2002; J. T. N. Young & Rees, 2013). Most studies have focused on youth, but although influence of and time spent with friends decreases in adulthood (e.g., Steinberg & Monahan, 2007), romantic partners may be more important for adults and adults have more freedom to select their own network members, which may result in more homogeneous networks (e.g., J. T. N. Young & Rees, 2013). For example, longitudinal research on the effect of offending and victimisation of social network members on the risk for offending and victimisation of Dutch adults, found support for selection and influence processes (Rokven et al., 2017; Rokven et al., 2016). Additionally, it has shown that not all contacts show the same similarity in deviance, as similarity is stronger for more important social contacts, who are contacted daily.

Extant cross-sectional quantitative research on cyber-offending has shown that in general cyber-dependent crime is more often committed if a person has friends who show cyber-deviant behaviour or attitudes as well (e.g., Bachmann, 2010; Bossler & Burruss, 2011; Donner, Marcum, Jennings, Higgins, & Banfield, 2014; Hollinger, 1993; Holt, 2007; Holt, Bossler, et al., 2012; Holt et al., 2010; Holt & Kilger, 2008; Hu et al., 2013; Marcum et al., 2014; Morris, 2011; Morris & Blackburn, 2009; Rogers, 2001; Skinner & Fream, 1997). In addition, qualitative studies showed that cyber-offenders share IT-knowledge, information on criminal opportunities, and neutralisation techniques, with online and offline friends and on forums (e.g., Holt, 2007, 2009a; Holt, Strumsky, et al., 2012; Hutchings, 2014; Hutchings & Clayton, 2016).

4.1.3 Limitations previous research on cybercrime

The existing evidence for similarity in cyber-offending in social networks should be interpreted with caution, as some studies include traditional cyber-enabled deviance or more socially accepted, and in The Netherlands only recently criminalised, deviance like online piracy. One reason that studies focus on these crimes that require fewer IT-skills and IT-use, could be that they use juvenile or college samples in which cyber-dependent offending is less common.

Another limitation of the quantitative research is that they mostly only focus on deviant behaviour of same-aged peers, while the qualitative research has shown that older social contacts with more authority can act as mentors in learning to use IT-skills for illegal purposes (e.g., Chiesa, Ducci, & Ciappi, 2008c; Holt et al., 2010; Skinner & Fream, 1997). In addition, previous research generally measures deviance of all peers in one item that reflects the overall presence of deviance in the peer network. Therefore, possible differences in the influence of social contacts, related to contact frequency or similarity in characteristics, have not been studied. In addition, these studies have not been able to control for similarity in other characteristics that could have influenced both the selection of friends and the similarity in deviance of friends. For example, young males have a higher likelihood of offending. If a person is young and male, he may be more likely to select friends who are also young and male. A relation between their behaviour may, therefore, be partly spurious.

Most importantly, previous research did not empirically compare the strength of similarity in deviance in social networks between cybercrime and traditional crime. Studies have focused on applying social learning to cybercrime, claiming that, for example, imitation may be more important for learning skills compared to traditional crime. Thereby missing arguments that could imply that there is less influence or selection for cybercrime.

4.1.4 Less similarity in cyber-deviance in strong social networks

Goldsmith and Brewer (2015) theorise that strong and face-to-face social contacts are less important for cyber-dependent criminal behaviour as learning is now possible through the internet, in a more self-directed way. Qualitative studies also show that although some hackers also have offline social contacts who hack, they mainly operate alone and learn their skills from internet sources like forums and by trial and error (Holt, 2007, 2009a). Even though the contents of these forums are posted by others, we argue that forums could more accurately be seen as sources of information rather than sources of social learning. A person can simply seek information on these forums in a self-directed way. Holt (2007) describes that even if a person asks for specific information on these forums, other users generally only post a link to a webpage that contains relevant information. This could mean that having strong social contacts who are deviant is less important for cyber-offenders, while strong contacts are most important in their influence on traditional offenders (e.g., Agnew, 1991; Rokven et al., 2017).

In addition, non-deviant social contacts may also have less influence on cyber-deviant behaviour. Several authors have theorised that the digital context changes behaviour, because of its anonymity and lack of connection with the "real" world (e.g., Jaishankar, 2009; Suler, 2004; Yar, 2013a). They argue that behaviour in this context is less visible and for people it feels like the online world is disconnected from the offline world. Because of this disconnect they think that their online behaviour does not have any offline consequences. In addition, apprehension rates for cybercrimes are very low (e.g., Leukfeldt et al., 2013; Maimon et al., 2014) and offenders may not be aware that what they are doing is actually illegal and their behaviour is crossing lines that they would not cross offline because of the negative social consequences (e.g., Jaishankar, 2009; Suler, 2004; Yar, 2013a). This could decrease the perception that these crimes will have any negative consequences on a person's social life. We argue that this lack of visibility of criminal behaviour and the perception that it will not affect social relationships can decrease the influence of social contacts.

For the same reason, a cyber-offender may not have to consider the attitudes of new social network members towards cyber-offending when selecting those network members. In addition, the invisibility of cybercriminal behaviour could decrease opportunities for selecting new deviant network members in real life, but as discussed above the availability of online information about the criminal use of IT-systems reduces the need for having social contacts with these skills (e.g., Holt, 2009a; Holt et al., 2010; Holt & Kilger, 2008). In sum, we argue that the digital context in which cyber-dependent crimes take place may reduce the effect of both influence and selection processes for cyber-deviant behaviour. If this is the case, there will be less similarity in deviance in social networks for cybercrime compared to traditional crime.

4.1.5 The current study

The arguments above call in to question to what extent the similarity in cyber-offending in social networks found in previous research, is just as strong as that similarity for traditional offending. We will address this by using data on core discussion networks from an online survey among a high risk sample of cybercrime and traditional suspects drawn from the prosecutors' office database in The Netherlands. This sample enables us to study less common cyber-dependent offending and compare this to traditional offending, in an understudied population of adult offenders, thereby addressing some of the gaps in the literature. Our main research question is:

1. *Is there a difference in the extent to which there is a relation between cyber-deviant behaviour of an individual and cyber-deviance of his/her social network members compared to that relation between traditional deviant behaviour and traditional deviance of network members?*

Based on previous cybercrime research we expect to find a relation between cyber-deviant behaviour of an individual and cyber-deviance of social network members (Hypothesis 1). On the other hand, based on the arguments provided in the previous section we expect that this relation is weaker for cybercrime compared to traditional crime (Hypothesis 2). To strengthen our conclusions, we will test if these estimates change statistically significantly when we include control variables for the similarity in gender and age between a person and a social network member. This will tell us to what extent this similarity in deviance may be spurious, because of selection effects based on gender or age.

Additionally, our ego-centred network data, that includes separate observations for the most important social contacts in a person's life, enables us to explore if cybercrime is comparable to traditional crime in the way the correlation between the behaviour of a person and the behaviour of social contacts differs between contacts. Hence we also explore:

2. *Are there differences in the extent to which there is a relation between cyber-deviant behaviour of an individual and cyber-deviance of his/her social network members for different social*

network members (daily/non-daily contacts, same gender/other gender, same age/older/ younger) and are these differences comparable to those for traditional deviance?

Based on previous research on traditional crime, we expect that the relation between deviant behaviour of an individual and deviance of social network members is stronger for daily contacted network members compared to non-daily contacted network members (Hypothesis 3). More contact indicates more selection and may increase the influence of a social contact. In addition, as a person may identify more with social contacts with similar characteristics and therefore may be more likely to socially learn that person's behaviour, we expect that the relation is stronger for network members of the same gender and age (Hypothesis 4).

4.2 Data and methods

4.2.1 Sample and procedure

For this study we selected all 1,100 cybercrime suspects and a random sample of 1,127 traditional suspects from the prosecutor's office database in the Netherlands for the period 2000-2013. Of this sample 928 cybercrime and 875 traditional suspects had a valid current mailing address and were invited by regular mail to participate in our study in the summer of 2015. The invitation letter included a web link and unique password that could be used to access an online survey. The letter included the option to complete the survey on paper (used by three traditional sample respondents) or through a Tor Hidden Service website[1] (used by three cybercrime sample respondents). The invitation letter also mentioned the scope of the study, confidentiality and anonymity, and the 50-euro voucher that respondents would receive in exchange for their participation. The first page of the survey included a consent form and further detailed the selection procedure, confidentiality, anonymity and the scope and content of the survey.

The response rate of traditional sample suspects was lower than the response rate of cybercrime sample suspects. As we aimed for two equally sized samples, we sent reminder letters after two and four weeks to the traditional suspects. After six weeks 268 cybercrime suspects (28.88%) and 141 traditional suspects (16.11%) had fully participated. To gain equal samples we invited a new sample of 781 traditional suspects following exactly the same procedure. After two reminders 126 of them (16.13%) participated and the final sample included 268 cybercrime suspects and 267 traditional suspects, response rates of respectively 28.88% and 16.12%.

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

4.2.2 Measures

Dependent variables

Cyber-offending and traditional offending were measured as two dichotomous variables (1 = offended). Respondents who self-reported to have committed at least one type of cybercrime or traditional crime in the preceding twelve months were considered to be a cyber-offender or traditional offender (see Table 4.1 for descriptive statistics of dependent and independent variables). Thirteen different types of cybercrime were included based on the Dutch National Cyber Security Centre (2012) list of cyber-dependent crimes and the Computer Crime Index of Rogers (2001). These included: hacking by guessing passwords (8.09%), digital theft (6.07%), defacing (5.78%), other types of hacking (5.20%), damaging data (4.05%), phishing (3.76%), taking control over an IT-system (3.47%), intercepting communication (2.31%), malware use (2.02%), DoS attacks (2.02%), selling somebody else's data (1.73%), spamming (1.45%), and selling somebody else's credentials (0.87%). Eleven types of traditional offending were included based on Svensson et al. (2013) and Dutch criminal law. These included: tax fraud (7.80%), stealing (5.78%), threats (5.49%), buying or selling stolen goods (4.91%), carrying a weapon (4.62%), violence (4.34%), vandalism (4.34%), selling drugs (3.76%), insurance fraud (3.47%), burglary (1.16%), and using a weapon (0.87%).

Table 4.1.
Descriptive statistics

Egos		Alters	
Dichotomous variables	**%**	**Dichotomous variables**	**%**
Cyber-offender	18.79	Cyber-deviant alter	8.85
Traditional offenders	21.97	Traditional-deviant alter	4.66
Non-Dutch	22.54	Daily contact alter	44.69
Male	77.46	Alter same gender as ego	59.96
Continues variables	**Mean**	Alter same age as ego	9.15
Low self-control	1.74	Alter younger than ego	43.92
IT-skills	4.47	Alter older than ego	46.94
Age[1]	36.81		
Level financial problems	0.23		
N	346	N	1,159

1: In the models age was subtracted by 17 to start at 0 and models included age, age-squared and age-cubic

Independent variables

Alters

By using a name-generator/interpreter method (McCallister & Fischer, 1978), our respondents, in this type of analyses called egos, were asked to name up to five important personal social network members, called alters, with whom they had discussed important things in the preceding twelve months. If desired, they could use fake names. These names were then used to ask respondents about cyber- and traditional deviance of the alter, contact frequency, age and gender of alter, and their relationship with alter. Among all egos who named at least one alter, the average number of alters was 3.35 (48.22% friends, 35.09% family members and 16.70% partners), 55.16% of the alters was male and they were on average 39.94 years old.

The cyber- and traditional deviance of an alter were measured by using two questions for both cybercrime and traditional crime. Alter's offending was measured asking *"As far as you know, did this person commit online (digital)/offline (non-digital) criminal offences in the past 12 months?"*, which could be answered by *"yes"* or *"no"*. Alters deviant attitudes were measured asking: *"In general, what does this person think about committing online (digital)/offline (non-digital) criminal offences?"*, which could be answered with *"Mostly approves it"*, *"Sometimes approves sometimes disapproves it"* or *"Always disapproves it"*. Examples of offences were provided, reflecting the crimes in the ego self-report questions. Alter was considered a cyber- or traditional deviant if he or she committed a cybercrime or traditional crime or mostly approves committing a cybercrime or traditional crime, which was analysed as a dichotomous variable (1 = deviant alter). The deviance of each individual alter could be related to the behaviour of ego, consequently we analysed each alter-ego combination as an individual observation.

Similarity of alters and ego was constructed by comparing the reported gender and age of alter with the gender and age of ego. Alters were classified as younger, exactly the same age, or older, and as same gender or different gender. For both research questions, the dichotomous variables on similarity in age and gender were included in additional analyses to test if the estimates changed statistically significantly. For the second research question, it was also measured if ego had daily contact with alter. This was based on three questions asking how often ego and alter met offline (in real-life), had contact through online text messages, and online or offline phone calls. If one of these questions was answered with daily, alter was considered to be a daily contact. For the second research question, the different alter classifications were used to include dichotomous main effects for different deviant alters compared to all non-deviant alters. For example, if the dichotomous variable "deviant alter – same age" equals 1 for cybercrime, alter is cyber-deviant and of exactly the same age as ego.

Egos

In addition to the deviance of alters, we included ego's low self-control and IT-skills. It is important to control for low self-control as it could potentially both influences the likelihood of offending and the likelihood of selecting deviant friends or being influenced by deviant friends, as argued by Gottfredson and Hirschi (1990). Even though empirical evidence for this notion is mixed (e.g., Boman, 2016; McGloin & Shermer, 2009; J. T. N. Young, 2011). Furthermore, analogous to traditional crimes (e.g., McGloin & Shermer, 2009; Pratt & Cullen, 2000; Pratt et al., 2009), studies have shown that low self-control is a predictor of cyber-dependent offending, even when social learning measures are included (e.g., Bossler & Burruss, 2011; Donner et al., 2014; Holt, Bossler, et al., 2012; Hu et al., 2013; Marcum et al., 2014). Low self-control was constructed with items from the HEXACO-SPI-96 personality inventory (De Vries & Born, 2013). We used the formula from Van Gelder and De Vries (2012) to construct HEXACO Self-Control, which is based on the scale developed by Grasmick et al. (1993). Van Gelder and De Vries (2012) used the formula: HEXACO Self-Control = (3*Prudence + 2*(Fairness + Modesty + Fearfulness + Flexibility) + (Social Self-esteem + Patience + Inquisitiveness + Diligence + Altruism))/16. The original Altruism item was not included in the HEXACO-SPI-96 we used, therefore we slightly modified the formula and used 15 instead of 16 items. Self-control was reverse coded to a continuous low self-control scale.

Previous research has claimed that the IT-skills needed to commit cybercrimes could be learned from deviant friends by imitation. Nevertheless, based previous findings it could be argued that not all of these deviant IT-skills are learned from social contacts, as IT-skills are still an important predictor of cyber-offending if social learning an low self-control measures are included (e.g., Holt, Bossler, et al., 2012; Holt et al., 2010; Morris & Blackburn, 2009). Therefore, it is important to include IT-skills of ego in our analyses as well, to see to what extent the relationship between ego's IT-skills and cyber-dependent offending is explained by the possibility of learning those IT-skills from deviant friends. IT-skills were measured with an objective IT-skills test, based on ten knowledge questions ranging from very easy, like *"Which of the following email addresses can be valid?"* 1. *"www.infobedrijfx.nl"* 2. *"info@bedrijfx.nl"* 3. *"https://www.infobedrijfx.nl"* 4. *"info@bedrijfx"* 5. *"I do not know"*, which was answered correctly by 92.49%, to very challenging like a piece of code that contained a bug and respondents had to indicate which techniques could be used to prevent misuse of this bug, which was answered correctly by 4.34% (see

Appendix A for all questions). The IT-skills measure used in this study reflects the number of right answers to these questions. This measure was strongly correlated to a subjective IT-skills measure (Pearson's r = .75, p < .001) that was also included in this survey, based on Holt, Bossler, et al. (2012).

Other control variables were gender (1 = male), age (age-17, and age-squared and age-cubic), ethnicity (1 = non-Dutch origin), and the level of experienced financial problems in the preceding twelve months (an adjusted version from The Prison Project; Dirkzwager & Nieuwbeerta, 2015). Respondents indicated if the following situations occurred (1 = yes): 1. *"saved money"* (reverse coded) 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 at my door"* 8. *"had debts of 5.000 euros or more"*. The sum of all items was divided by eight to obtain a scale from 0-1 (α = 0.83). In addition, we controlled for initial differences between the groups of cybercrime and traditional suspects with a dichotomous initial group variable (1 = same group as outcome variable). This will make sure that the estimates are not driven by initial differences between the groups in both the likelihood of a type of offending and, for example, the likelihood of having cyber-deviant contacts or IT-skills.

4.2.3 Non-Response and analytical strategy

Only the 364 respondents (68.04%) who named at least one social network member could be analysed. From these respondents, 18 respondents (4.95%) were excluded because of missing values on one of the dependent variables, resulting in a final sample of 346 respondents, 178 cybercrime and 168 traditional suspects. For traditional suspects, females were overrepresented among respondents (20.83% females among respondents compared to 13.84% in the original sample, $\chi^2(1) = 5.93$, $p < 0.05$). No other statistically significant differences in gender or age were found between respondents and non-respondents in the non-response analyses. For both cybercrime and traditional crime, respondents who named at least one social network member were slightly more delinquent compared to respondents who did not name a social network member, but these differences were not statistically significant (cybercrime: 15.09% versus 18.79%; traditional crime: 15.09% vs. 21.97%).

For analysing our cross-sectional data with binary outcome variables, we used logit models. As we analysed each alter-ego (N = 1,159) combination as an individual observation, we used clustering to adjust the standard errors for the within ego dependency of the observations. For between and within model comparisons 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.

We used the Multivariate Imputation by Chained Equations (MICE) procedure of STATA 12 (based on Royston, 2004) to multiply impute missing values on the independent variables of 268 observations (ego-alter combinations, 23.12%). In line with Von Hippel (2007) cases with missing values on the dependent variables were used in the imputation, but excluded from the analyses in this paper. We multiply imputed 20 datasets, which were used in estimating the models, while adjusting the coefficients and standard errors for the variability between imputations, by using the combination rules of Rubin (1987).

4.3 Results

Results regarding our first research question can be found in Table 4.2 and are presented as odds ratios. These odds ratios show how many times the odds that a person committed a crime are higher if the independent variable changed by one unit, for example if the alter is deviant. The last column shows the statistical comparison between the estimates for cybercrime and traditional crime. The most important finding of this study is that, although we find a statistically significant positive relation between cyber-deviance of social network members and a person's cyber-dependent criminal behaviour, in line with hypothesis 1, this relation is statistically significantly weaker for cyber-offending compared to traditional offending, in line with hypothesis 2. Where the odds that a person committed a traditional crime are 10.67 times higher when a social contact is deviant, the odds that a person committed a cybercrime are only 2.46 times higher when a contact is deviant. Additional analyses indicated that these estimates barely (and not statistically significantly) changed when similarity in age and gender were included[2].

In addition, we find that more IT-skills and low self-control are also positively related to cyber-offending. Low self-control is also statistically significantly related to traditional offending and although the effect of low self-control is larger for cybercrime, the difference is not statistically significant. For traditional crime there is no effect of IT-skills, while a one-unit increase in IT-skills increases the odds that a person committed a cybercrime by 1.30. This is statistically significantly different between cybercrime and traditional crime. Overall the estimates of the models for cybercrime and traditional crime are statistically significantly different from

[2] Results can be requested from the first author.

each other ($F(10) = 1.90$, $p < .05$). Although the relation between deviance of social contacts and offending is statistically significantly stronger for traditional crime, the overall model including IT-skills and low self-control has more explanatory power for cybercrime (average pseudo R square over imputed data: cybercrime 0.17. traditional crime 0.10). Additional analyses showed that these results are robust when excluding the IT-skills and/or initial group variables, which indicates that the strength of the result for cyber-deviant social contacts is not affected by the inclusion of IT-skills measures. In addition, robustness-checks, in which we systematically excluded one of the cybercrime or traditional crime types from the analyses, showed that the results were not driven by one type of crime and other robustness analyses indicated that there were no meaningful differences between friends and other contacts[3].

Table 4.2.
Clustered alter-ego logit models for cyber- and traditional offending of ego

	Cybercrime			Traditional crime			Comparison
	OR	B	SE	OR	B	SE	F(df)
Deviant alter[1]	2.46*	0.90	0.41	10.67***	2.37	0.45	5.81(1)*
IT-skills	1.30***	0.26	0.08	0.99	-0.01	0.07	8.71(1)**
Low self-control	3.04**	1.11	0.35	1.98*	0.68	0.33	1.07(1)
Financial problems	1.15	0.14	0.60	1.87	0.63	0.56	0.54(1)
Male	0.64	-0.45	0.41	1.09	0.09	0.35	1.69(1)
Non-Dutch	1.33	0.29	0.38	1.26	0.23	0.33	0.02(1)
Age							2.09(3)
Age	0.76*	-0.28	0.11	0.96	-0.04	0.09	3.51(1)
Age-squared	1.01	0.01	0.01	1.00	0.00	0.00	1.99(1)
Age-cubic	1.00	0.00	0.00	1.00	0.00	0.00	1.17(1)
Initial group[2]	1.71	0.53	0.38	1.26	0.23	0.32	0.29(1)
R square[3]			0.17			0.10	

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

N (alter-ego) = 1,159

1. For the cybercrime model this reflects the estimate for a cyber-deviant alter, for the traditional crime model this reflects the estimate for a traditional deviant alter.
2. 1 = same initial group category as outcome variable category.
3. Average pseudo R square over imputed data

[3] Results can be requested from the first author.

Results regarding our second research question can be found in Table 4.3. For cybercrime, the similarity in deviant behaviour is stronger for social contacts who are contacted daily, of the same gender as ego, and older than ego. For contact frequency and gender, we see similar patterns for both cybercrime and traditional crime, in line with hypotheses 3 and 4. However, with respect to age similarity, we see that the results point in the direction of opposite effects for cybercrime and traditional crime. While older cyber-deviant social contacts show the strongest and only statistically significant relation with cyber-offending, in contrast with hypothesis 4, they show the weakest relation with traditional offending. Similarly, same-aged social contacts are most important for traditional offending, in line with hypothesis 4, while they are the least important for cyber-offending. Overall and in line with hypothesis 2, these models show that the similarity in deviant behaviour of all social contacts is stronger for traditional crime. These estimates also did not change statistically significantly when similarity in age and gender were included as control variables[3].

Table 4.3.
Deviant alter estimates for different alters

	Cybercrime			Traditional crime			Comparison
	OR	B	SE	OR	B	SE	F(df)
Deviant alter[1]	2.46*	0.90	0.41	10.67***	2.37	0.45	5.81(1)*
Deviant alter - daily contact	2.73*	1.00	0.51	12.26***	2.51	0.66	3.54(1)
Deviant alter - non-daily contact	2.18	0.78	0.54	9.31***	2.23	0.67	2.66(1)
Deviant alter - same gender	3.02**	1.11	0.42	12.00***	2.48	0.53	3.81(1)
Deviant alter - other gender	1.36	0.31	0.72	8.18**	2.10	0.81	3.58(1)
Deviant alter - same age	1.61	0.47	0.62	26.08**	3.26	1.06	5.67(1)*
Deviant alter - younger	2.04	0.71	0.55	11.77**	2.47	0.84	2.86(1)
Deviant alter - older	4.00**	1.39	0.54	7.59***	2.03	0.58	0.87(1)

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

1. For the cybercrime model this reflects the estimate for a cyber-deviant alter, for the traditional crime model this reflects the estimate for a traditional deviant alter.

Note: all estimates reflect the effect of a deviant alter compared to all non-deviant alters. For example, for daily contact the estimate 'deviant alter - daily contact' reflects the estimate of a deviant alter who is contacted daily compared to all non-deviant alters, both daily and non-daily contacted alters.

Note: Models included all variables from the original model. This table only shows the variables of interest. Complete models can be requested from the first author.

It should be noted, however, that there were no statistically significant differences between the estimates for different social contacts, for both cybercrime and traditional crime[4]. As an example, although the odds ratio for a same-gender cyber-deviant contact is 3.02 and the odds ratio for an other-gender cyber-deviant contact is only 1.36, the strengths of these estimates do not differ statistically significantly ($F(1) = 1.29$, $p = .26$). This means that we do not find statistically significant evidence for hypotheses 3 and 4. Nevertheless, apart from the difference with respect to older cyber-deviant social contacts discussed above, the results point in the direction of these hypotheses.

4.4 Conclusion and discussion

In this paper we focused on cyber-dependent crimes that are completely committed in the anonymous digital context of IT-systems, where there are no physical social interactions (e.g., Jaishankar, 2009; Suler, 2004; Yar, 2013a) and IT-skills and knowledge on how to use those skills illegally are essential in committing crimes in this context (Holt et al., 2010). Based on the distinct criminal setting of these crimes we argued that the relation between deviant behaviour of an individual and the deviance of social network members would be weaker for cybercrime compared to traditional crime. We tested this hypothesis by using ego-centred network data on core discussion networks from an online survey among a high risk sample of cybercrime and traditional former suspects in The Netherlands. We contributed to the literature on cybercrime by specifically addressing less common cyber-dependent offending and comparing these to traditional offending in an understudied population of adult offenders. In contrast to previous research we studied the most important social contacts, not only same-aged peers, and we compared differences based on contact frequency and similarity between social contacts.

In line with previous studies on cybercrime, we found that there is a statistically significant relation between cyber-deviance of social network members and cyber-dependent criminal behaviour of a person, even when controlling for similarity in age and gender between a person and a social network member. Nevertheless, our findings put previous results on cybercrime in perspective, as the comparison clearly showed that, in line with our expectations, the relation is weaker for cybercrime compared to traditional crime. This could mean two things, (1) compared to traditional offenders, cyber-offenders do not need strong social contacts who are deviant to commit cybercrimes as much as traditional offenders

[4] Results can be requested from the first author.

need them to commit traditional crimes (e.g., Goldsmith & Brewer, 2015), and/or (2) cyber-offenders do not consider their contacts' negative or positive social reactions as much when they commit crimes in the digital context (e.g., Jaishankar, 2009; Suler, 2004; Yar, 2013a). In other words, social contacts may have less influence on deviant behaviour online, and/or people may not consider the attitudes of new social contacts towards online deviant behaviour when selecting them. Our results show the value of examining cybercrime in comparison to traditional crime when applying traditional theories to cybercrime. In that way, differences in the strength of correlates can indicate to what extent social network based prevention strategies designed for traditional crime, are expected to have a similar effect on cybercrime. This type of comparison makes the large body of research on traditional crime also more useful in understanding cybercrime.

In addition to our major finding, IT-skills were strongly related to cyber-offending. This shows that not all IT-skills that are needed for cyber-offending are learned from strong social contacts, for example by imitation, and in combination with the weaker similarity in deviant behaviour, this indicates that IT-skills are also learned in another way, for example by reading information online (e.g., Goldsmith & Brewer, 2015; Holt, 2007, 2009a; Holt et al., 2010; Holt & Kilger, 2008). Still, as there is a small but statistically significant relation between deviant behaviour of strong social contacts and cyber-offending, future longitudinal research could further investigate which specific selection or influence processes underlie this relation and in what way learning IT-skills is related to cyber-offending. Such a study could also include traditional offending, as that will further inform us about the way the digital context of cybercrime has changed processes of selection and influence.

In addition to the comparison our data-structure enabled us to explore differences in the similarity in behaviour between different social contacts. In our sample the estimates for different social contacts did not differ statistically significantly from each other for both cybercrime and traditional crime. However, the results pointed in the direction of our expectation that the relation is stronger for daily contacted contacts of the same gender. Most importantly though, the results indicated that for cybercrime the relation is stronger for older social contacts, while for traditional crime these show the weakest relation. So in addition to a weaker similarity in deviant behaviour, cyber-deviance also seems to be the result of different social processes with different social contacts. This is in line with previous studies on cybercrime that have shown that older mentors can be important in a social learning process for cybercrime (e.g., Chiesa et al., 2008c; Holt et al., 2010; Skinner & Fream, 1997). This therefore indicates that future studies could not only focus on same-aged peers, but also on other social network members that can influence a person's behaviour.

The future research recommendations above should preferably be studied in longitudinal designs, as that enables distinguishing selection and influence processes, and could shed light on how people acquire IT-skills and knowledge on illegal use of those skills over time. It has been shown in the past that the effect of deviant peers slightly differs between different types of cybercrime (e.g., Morris & Blackburn, 2009). We focused more specifically on thirteen different cyber-dependent crimes instead of a broader outcome variable that also includes cyber-enabled crime. Nevertheless, even within this group of cyber-dependent crimes, there may be differences in peer-effects. In addition, we compared this specific type of cyber-offending with a broad category of traditional offending. This addresses the most fundamental research question about differences between cybercrime and traditional crime with respect to peer-effects. Nevertheless, future studies with larger samples and prevalence rates could benefit from both comparing different types of cyber-dependent crime and different types of traditional crime. In addition to prevalence rate restrictions, our study did not allow for differentiating in the outcome variable, because we only asked about online and offline deviance of each social network member in general, without differentiating between different types of online or offline deviance.

If future studies are able to distinguish selection effects from influence effects, these studies could further focus on the explanatory power of different components of social learning (e.g., differential association, deviant definitions, imitation and reinforcement; Akers, 1998). Some previous studies, for example, suggest that imitation is more important for cybercrime as it can be a way to learn IT-skills (e.g., Holt et al., 2010). However, this claim is not in line with our finding of a weaker similarity in deviant behaviour for cybercrime and the consistent finding that IT-skills still predict cyber-offending when deviance of social contacts is included in the analyses (e.g., Holt, Bossler, et al., 2012; Holt et al., 2010; Morris & Blackburn, 2009). In addition, future longitudinal studies will be able to test to what extent low self-control predicts who is influenced by social contacts or who will select deviant social contacts.

The present study also had several limitations that merit discussion. The cross-sectional nature of our data did not enable us to distinguish between selection and influence processes. In addition, studies have shown that when asking people to indicate the deviance of their social network, they may project their own behaviour on their network members, which results in an overestimation of similarity within social networks (e.g., Boman, Rebellon, & Meldrum, 2016; Weerman & Smeenk, 2005; J. T. N. Young, Rebellon, Barnes, & Weerman, 2014). For cybercrime it may be even harder to know actual behaviour and attitudes of contacts, as their online behaviour is less visible, which may reduce their influence on offending. However, in contrast, prevalence rates of deviance among social contacts were higher for cyber-deviance compared to traditional deviance. In addition, in line with previous research (e.g., Rokven et al., 2016), we see much higher levels of self-reported offending than perceived deviance of social contacts for both cybercrime and traditional crime. Nevertheless, it is important that future studies use a social network method as the one used in Weerman and Smeenk (2005), where the network members report on their deviant behaviour themselves. This would increase our knowledge on people's ability to know about their social contacts' cyber-deviance and the differences between similarity in perceived and actual deviance in social networks for cybercrime. It would also be advisable to measure co-offending in these networks, to see to what extent people know about each other's cyber-deviance because they committed cybercrimes together.

Making a meaningful comparison between less common cyber-dependent crime and traditional crime requires the use of high risk samples from the same source, but this sample frame limits the generalisability of our results. As all respondents were suspected of a crime prior to the twelve-month period of the self-report questions, the results reflect the difference in presence of current deviant social contacts among offenders who have not been deterred by police contact, in comparison to offenders who have not committed crimes in the preceding twelve months. Furthermore, as our respondents have not been able to avoid the long arm of the police, this may indicate that they have fewer skills to hide their crimes, than offenders who have not been caught. Similarly, our Dutch sample may also impact the level of IT-skills of offenders, as some say that highly skilled offenders originate from other countries (e.g., Chua & Holt, 2016; European Cybercrime Center, 2014; Holt & Kilger, 2012). In other words, the results may be different in the general population, among first offenders, or in other countries. Still, for future research, longitudinal full network studies for cyber-dependent crimes could most likely not be conducted in general population samples, because of the low prevalence of these cyber-dependent crimes.

Despite the limitations, our findings may make us wonder whether the increasing presence in the digital world, may further change social laws that have always predicted behaviour. This challenges the use of known social processes in interventions against undesirable behaviour in the future, especially if this behaviour moves more and more to the digital world, thereby further reducing connections to the physical world. In sum, this study suggests that theories and established research findings, like similarity in deviant behaviour in social networks, cannot always be assumed to be equally applicable to cyber-dependent offending. Even though there is a relationship between the cyber-deviant behaviour of social network members this is weaker than the relationship for traditional deviant behaviour, which can have important implications for prevention strategies that focus on the social network if these findings are replicated in future comparisons in different samples.

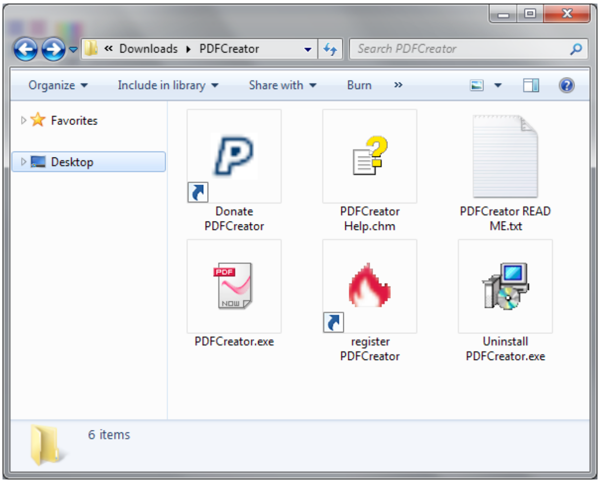
4.5 Appendix A: IT-skills test

Some items are inspired by online IT-skills tests, others were formulated with the help of the Dutch High Tech Crime Team of the National Police. After data collection ended the High Tech Crime Team also helped evaluating the given answers, which resulted in accepting some extra answers as being correct.

Explanation provided for respondents:

The next questions are about your knowledge on computers, ICT-systems and the internet. It does not matter if you do not know the answer to a question, we are interested in your knowledge and therefore we ask you to answer **without the help of others** and **without looking up the answers**. If you do not know the answer, you can check the “I do not know” box.

Question 1:



You downloaded the program PDFCreator and you want to use it right away.

You should double click on one of the icons above, which one?

1: PDFCreator Help.chm

2: PDFCreator READ ME.txt

3: PDFCreator.exe

4: Uninstall PDFCreator.exe

98: I do not know

Right answer: 3 (83.24%)

Question 2:

What encoding is most likely used in the string below and what does it say without encoding?

“YmFzZTY0IG5hdHV1cmxpamshCg==”

1: The encoding used is: base64

Without encoding is says: “base64 natuurlijk!”

2: The encoding used is: uuencoding

Without encoding is says: “uuencoding is gaaf”

3: The encoding used is: base64

Without encoding is says: “waarom geen base64?”

4: The encoding used is: yenc

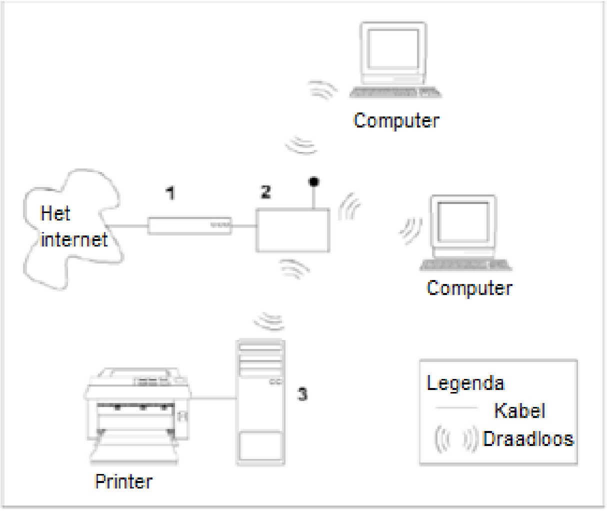
Without encoding is says: “wordt usenet nog gebruikt?”

98: I do not know

Right answer: 1 (12.43%)

Question 3:

The picture below shows an office network:



Which of the following descriptions describe the devices most accurately?

1: Device 1 is a Broadband modem; Device 2 is a Wireless router; Device 3 is a Wireless printer server

2: Device 1 is a Wireless router; Device 2 is a Broadband modem; Device 3 is a network fileserver

3: Device 1 is a Network fileserver; Device 2 is a Hub; Device 3 is a Wireless printer server

4: Device 1 is a Broadband modem; Device 2 is a Wireless print server; Device 3 is a Wireless router

98: I do not know

Right answer: 1 (67.34%)

Question 4:

In MySQL, where is de metadata saved?

1: In the MySQL database “mysql”

2: In the MySQL database “metadata”

3: In the MySQL database “metasql”

4: None of the answers above is correct

98: I do not know

Right answer: 1 or 4 (19.65%)

Question 5:

Which of the following email addresses can be valid?

1: www.infobedrijfx.nl

2: info@bedrijfx.nl

3: https://www.infobedrijfx.nl

4: info@bedrijfx

98: I do not know

Right answer: 2 or 4 (92.49%)

Question 6:

Below are statements, which of these statements is/are correct?

Statement 1: Virtual Machines are used for making the best use of available hardware

Statement 2: Virtual Machines are an easy way to separate different users

Statement 3: In a Virtual Machine you are protected against malware

1: statement 1 is correct

2: statement 2 is correct

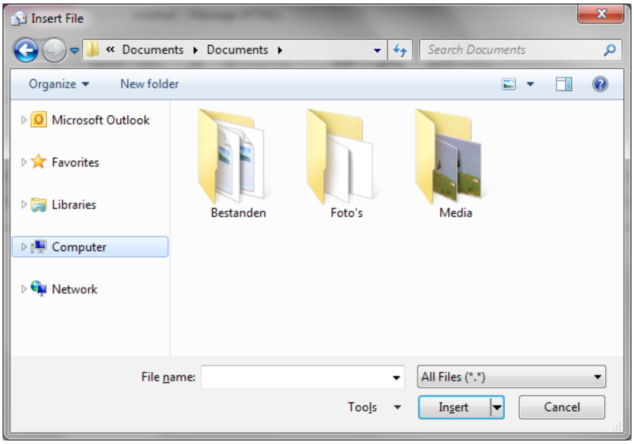
3: statement 1 and 2 are correct

4: statement 2 and 3 are correct

98: I do not know

Right answer: 1 or 3 (36.42%)

Question 7:



Imagine you want to attach the folders above to an e-mail.

What is the best way to do this?

1: Select all three folders and click on insert

2: Zip all folders to a ".zip" folder, select that folder and click on insert

3: Click on "All Files" and select the file type "folder", select all folders and click on insert

4: Open all folders, select all files in the folders and click on insert

98: I do not know

Right answer: 2 (49.13%)

Question 8:

Which of the following websites uses encryption?

1: www.webshop.nl/secure

2: http://www.webshop.nl/secure

3: https://www.webshop.nl/secure

4: httpv://www.webshop.nl/secure

98: I do not know

Right answer: 3 (54.34%)

Question 9:

In what order are webpages loaded?

1: URL => IP => DNS

2: IP => DNS => URL

3: URL => DNS => IP

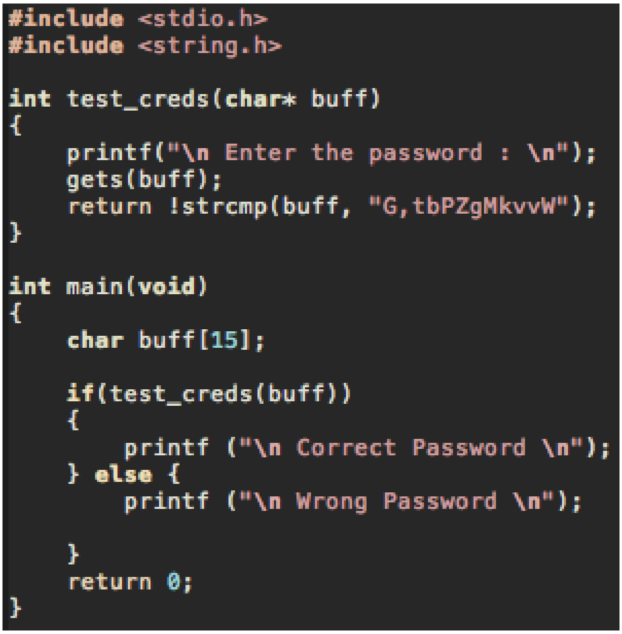
4: IP => URL => DNS

98: I do not know

Right answer: 3 (28.03%)

Question 10:

In the code below it is possible to execute your own code.



```
#include <stdio.h>
#include <string.h>

int test_creds(char* buff)
{
    printf("\n Enter the password : \n");
    gets(buff);
    return !strcmp(buff, "G,tbPZgMkvvW");
}

int main(void)
{
    char buff[15];

    if(test_creds(buff))
    {
        printf ("\n Correct Password \n");
    } else {
        printf ("\n Wrong Password \n");

    }
    return 0;
}
```

Which of the techniques below is not suitable to hinder and/or prevent this kind of misuse?

1: PaX

2: Taint checking

3: SEH

4: ASLR

98: I do not know

Right answer: 3 (4.34%)

Chapter 5

Cybercrime versus traditional crime: empirical evidence for clusters of offences and related motivations*

* This chapter was submitted as: Weulen Kranenbarg, M. (under review). Cybercrime versus traditional crime: empirical evidence for clusters of offenses and related motivations.

Abstract

Cybercriminal opportunities are increasing, but it is unknown to what extent the rise in these opportunities has resulted in distinctly different types of offenders with different motivations. In this study this question will be addressed by examining to what extent cyber-dependent offenders can be distinguished from traditional offenders, and identifying clusters of cyber-offences and traditional offences. In addition, it will be explored which motivations for offending the offenders provide and to what extent a specific cluster distinguishes itself from the other clusters by specific motivations. The analyses will be based on a survey among a high risk sample of adult cyber-offenders and traditional offenders (N = 508) registered by the Dutch public prosecutors' office. The principal component analysis identified seven clusters of crimes, four clusters that include only cybercrimes and three clusters that only include traditional crimes. This indicates that cyber-offenders can be distinguished from traditional offenders. In addition, cybercrimes can be distinguished from traditional crimes by almost all motivations. The cybercrimes are mostly committed out of intrinsic motivations, which means that committing the crime is in itself rewarding. Financial motivations are almost absent for cybercrime. Differences between cybercrime clusters are mainly found in extrinsic motivations, the extent to which the external consequences of committing a crime are rewarding. The results will be compared to the existing theoretical and limited empirical literature on cybercrime.

Keywords
cyber-dependent crime
motivations,
cybercrime clusters
traditional crime clusters
comparison

5.1 Introduction

The prevalence of cyber-dependent crimes[1] (for a detailed description of these crimes, see next section) is increasing (e.g., Grabosky, 2017; White, 2013) and it has been claimed that more and more cyber-offenders started to commit these crimes for financial gain, while increasingly less offenders commit them out of intrinsic motivations, driven by internal rewards (e.g., Chan & Wang, 2015; Grabosky, 2017; Holt & Kilger, 2012; Kshetri, 2009; Provos, Rajab, & Mavrommatis, 2009; Smith, 2015; White, 2013). These claims, however, are mostly based on the observation that opportunities for financial cybercrime have increased. Empirical offender-based studies on the relative importance of different motivations for cyber-dependent offending are almost absent. Similarly, it is unknown to what extent the increase in cybercriminal opportunities has resulted in distinctly different types of offenders with different motivations. Nevertheless, while cyber-offenders could theoretically be very different from traditional offenders, the existing empirical literature has focused on either cyber-offenders or traditional offenders, without comparing them. Lastly, for cyber-offenders the theoretical literature has indicated some offender typologies based on skills and motivations, but empirical evidence for these is also lacking.

In this study, these gaps in the literature will be addressed, first by examining to what extent cyber-dependent offenders can be distinguished from traditional offenders, and analysing which clusters of cyber-offences and traditional offences are generally committed by the same offenders. Second, it will be explored which motivations for offending the offenders provide and to what extent the clusters can be distinguished from the others by these motivations. The analyses will be based on data from a survey among adult cyber-offenders and traditional offenders (N = 508) registered by the Dutch public prosecutors' office.

5.1.1 Cyber-dependent crime

Different names and definitions for cybercrime are used in the literature, but in general a distinction is made between cyber-enabled and cyber-dependent crime (e.g., Furnell, 2002; Gordon & Ford, 2006; McGuire & Dowling, 2013; Wall, 2001; Zhang et al., 2012). Cyber-enabled crime refers to traditional crime in which Information Technology (IT) is used in the commission of the crime, for example, online fraud, stalking, harassment, and so on. This study, however, focuses on cyber-dependent crime, for example, hacking, web defacement, malware use,

[1] In this paper 'cyber-dependent crime' and 'cybercrime' will be used interchangeably to refer to these crimes.

and so on. These crimes cannot be committed without using IT, and therefore are theoretically very different from all other crimes. IT is the key element, as these crimes completely take place in a digital context and require IT-skills. It is unclear to what extent cyber-dependent offending can empirically be distinguished from all other types of offending. Offenders may combine cyber-offences and traditional offences, as some have argued that offenders combine different types of cybercrime or cybercrimes and traditional crimes, because those crimes can be part of a sequence of crimes, that are part of one modus operandi (Alleyne, 2011; Stephenson & Walter, 2012).

Some hypothetical distinctions within the overall category of cyber-dependent crimes have also been described. These distinctions are usually based on the way these crimes are committed. McGuire and Dowling (2013), for example, distinguished intrusions into computer networks (i.e., hacking), disruption or downgrading of computer functionality and network spaces (i.e., malware and denial-of-service (DoS) attacks), and spamming. These could all be further used for other means like stealing personal data. Hacking could additionally be used for defacing websites or as the start of a DoS attack, for example. Similarly, malware could be used for deleting files or crashing systems. In contrast, Kirwan and Power (2013) described infiltration, defacements, and DoS attacks as types of hacking, but malware as a different category. They theorised that malware is a form of vandalism, with motivations similar to traditional vandalism. Limited empirical evidence for such distinctions has been found in interviews with hacker conference attendees, which have indicated that phishers, spammers and virus coders are different from hackers (Bachmann & Corzine, 2010).

5.1.2 Typologies of hypothetical offenders and motivations

In addition to the hypothetical offence clusters that are based on the way crimes are committed, discussed above, some theoretical literature has distinguished hypothetical types of offenders based on their perceived motivations and skills. Most of this literature is about hackers (e.g., Alleyne, 2011; Dalal & Sharma, 2007; Kilger, Arkin, & Stutzman, 2004; Kirwan & Power, 2013; Rogers, 2000, 2006), but some articles also include other types of cyber-offenders (e.g., Furnell, 2002; Ibrahim, 2016; Nykodym et al., 2005; Parker, 1983; Wall, 2001). The hacker taxonomy of Rogers (2000, 2006) is well known and often cited. Rogers identified nine hypothetical hacker categories based on skill level and motivation (i.e., revenge, financial, curiosity, notoriety). He argued that this model can be used to show interactions and relative importance of motivations for different types of hackers and show progression of skill and motivation over time.

As Morris (2011) showed, the literature on offender categories and motivations discussed above is largely based on assumptions and anecdotal evidence. Empirical evidence for different types of cyber-offenders and their motivations is almost non-existent. The assumed motivations are generally based on the outcome of a crime. For example, if the victim suffers financial loss, the offender is often assumed to be motivated by financial gain (e.g., Kilger, 2011; Kilger et al., 2004; Leukfeldt, Lavorgna, & Kleemans, 2016; McGuire & Dowling, 2013; Randazzo et al., 2005; Tcherni et al., 2016). However, even if a crime causes financial loss, it may be motivated by other factors such as revenge and multiple motivations may underlie involvement in the attack (e.g., Holt & Kilger, 2012; National Cyber Security Centre, 2016; Rogers, 2006; Seebruck, 2015). Therefore, it can be more informative to study the different criminal offences that are generally committed by the same offenders and identify to what extent different motivations play a role in those offences.

When combining the existing theoretical literature (e.g., Chan & Wang, 2015; Chiesa, Ducci, & Ciappi, 2008d; Grabosky, 2017; Holt & Kilger, 2012; Kshetri, 2009; Provos et al., 2009; Smith, 2015; White, 2013), it could be concluded that intrinsic motivations are most important for cybercrime, while extrinsic motivations are less important, and financial motivations are argued to be becoming more important. For intrinsically motivated crimes, committing the crime is in itself rewarding. Intrinsic motivations are, for example, learning something from hacking into an IT-system, or acting out of curiosity, for the challenge, because it feels good, or to see how far one can go in misusing a system. Extrinsically motivated crimes are committed because the external consequences of committing that crime are rewarding. Extrinsic motivations are, for example, impressing others, delivering a message, wilfully damaging something that belongs to somebody else, or when you act out of revenge, anger or to bully someone. In comparison to traditional crime, Grabosky (2000, 2001) and Grabosky and Walkley (2007) claimed that most motivations for committing crimes are similar, but the intellectual challenge of defeating a complex system is probably unique for cybercrime. Nevertheless, empirical evidence on the extent to which these different or similar motivations are important and prevalent is scarce.

5.1.3 Empirical evidence on motivations

The limited empirical work done so far mostly focused on identifying all possible motivations for cyber-offending. In the Hacker Profiling Project (Chiesa et al., 2008a), for example, it was found that the worldwide online survey data of 216 hackers could identify different types of criminal hackers, that were also identified in the theoretical literature, with the following motivations: curiosity, learning, selfishness, anger, it is the in thing to do, media attention, prove power, financial gain. A decade before this project, Taylor (1999) already interviewed hackers[2] and identified six motivations: feelings of addiction, urge of curiosity, boredom with the educational system, feelings of power, peer recognition, and political acts. In one way or another, these are the motivations that are identified in the existing theoretical and empirical literature.

In line with the theoretical literature, there is empirical evidence for the relative importance of intrinsic motivations. Holt (2007), for example, showed in interviews and analyses of hacker forums that most hackers have a desire to learn and act out of curiosity. Similarly, studies showed that some hackers keep looking for new challenges. Their motivation is based on breaking a tougher system every time, thereby improving their skills(e.g., Voiskounsky & Smyslova, 2003; Woo, 2003).

Nevertheless, some types of cybercrime seem to be mostly intrinsically motivated while others are not. For example, Gordon and Ma (2003) compared their sample of criminal hackers to their previous work on malware writers and found that while most hackers are self-motivated and self-centred, virus writers are mostly motivated by peer recognition. In research on DoS attacks and web defacements, content analyses identified hacktivism, religiously motivated offenders or other types of motivation in which the offender tries to make a statement or deliver a message (Denning, 2011; Holt, 2009b). But, in contrast, in their analyses of web defacements, Woo et al. (2004) showed that only a few are politically motivated, as the majority are just simple pranks.

In addition to intrinsic motivations, some literature has suggested the importance of impressing others. On online forums, for example, hackers may gain status and respect (e.g., Holt, 2007; Nycyk, 2010). However, as these studies are based on forum posts they only reflect the perceived motivations of people who actually post on these forums. In addition, it is possible that the social status is not the initial motivation for offending, but only a motivation to talk about it on a forum afterwards (Jordan & Taylor, 1998). For example, Woo (2003) showed that intrinsic and extrinsic motivations are not mutually exclusive. While hacking may be intrinsically rewarding, the status that a hacker receives as a result of it is extrinsic. Yet, the intrinsic motivation was the initial motivation. Similarly, based on a literature review, and debriefs with young cyber-offenders known to the National Crime Agency of the United Kingdom, the NCA concluded that the challenge and

[2] It should be noted that not all literature about hackers is necessarily only about offenders. Hacking can be part of a completely legitimate profession.

accomplishment of cyber-offending is the main motive, but proving oneself to peers was important (National Crime Agency, 2017a, 2017b). In that study, financial gain was generally not a motive or only a secondary motive.

In 1999, financial motivations were not identified by Taylor (1999), but more recent studies too indicate that hacking is rarely committed for financial gain (Holt & Kilger, 2012; Turgeman-Goldschmidt, 2008). There have been studies based on Dutch criminal case files about the increase of financial motivations, but those yielded contradictory conclusions. A report of the Dutch police (Bernaards, Monsma, & Zinn, 2012), for example, showed that challenge or status is no longer an important motivation, while financial motivation is, in addition to 'delivering a message' through hacking or DoS attacks, and simple fun. In contrast, Leukfeldt et al. (2013) could not verify the shift from 'hacking for fame' to 'hacking for fortune'. Some commit it for profit, but revenge and curiosity were important motivations as well. They argued that this is because nowadays hacking could be committed by everyone and as a result more general motivations like revenge are getting more important. In contrast, based on interviews with Israeli hackers Turgeman-Goldschmidt (2008) argued that most hackers have a not-for-profit motivation and this will not change even given the fact that the nature of cybercrime constantly changes. In addition, some empirical evidence has suggested that young offenders are mostly intrinsically motivated, while later in their career most older offenders shift to committing crimes for financial gain (Bachmann, 2011; Bachmann & Corzine, 2010; Xu et al., 2013), although the opposite has also been found (Fotinger & Ziegler, 2004).

5.1.4 Justifications or neutralisations

It should be clear that examining motivations after a crime is committed is to some extent asking the offender's justification for offending (e.g., Bernasco, 2010b; Taylor, 1999; Yar, 2005b, 2013b). In retrospect it is not possible to reliably identify the motivations at the moment the crime was committed. Therefore, it is worth mentioning research on neutralisation techniques (Sykes & Matza, 1957) and justifications. Some neutralisation techniques that have been found among cyber-offenders are denial of victim (e.g., Morris, 2011; Turgeman-Goldschmidt, 2009), denial of injury (e.g., Chua & Holt, 2016; Morris, 2011; Turgeman-Goldschmidt, 2009), denial of responsibility (e.g., Chua & Holt, 2016; Hutchings & Clayton, 2016) and condemnation of the condemners (e.g., Turgeman-Goldschmidt, 2009). These seem to indicate that the digital context of cybercrimes makes it easy to deny the impact of a crime, as the consequences are not directly observable.

More useful in relation to motivations, however, may be that Turgeman-Goldschmidt (2009) found that most interviewed Israeli hackers also appeal to higher loyalties and self-fulfilment, which means they say to have committed the crimes because they want to keep learning and because they want to do the impossible. This is in line with the more intrinsic motivations mentioned in the literature as well. Based on the same interviews, Turgeman-Goldschmidt (2011) also argued that hackers cannot be compared to white-collar offenders as they generally do not commit their crimes for financial gain or out of extrinsic motivations or neutralisations. Appeals to higher loyalties have also been found among malware users (Chua & Holt, 2016) and booters (Hutchings & Clayton, 2016), who generally also say they do not provide their services for financial gain. Similarly, 127 criminal hackers who were interviewed at Defcon say they believe their actions serve a higher goal and improve security (R. Young et al., 2007).

5.1.5 The current study

With survey data of adult cyber-dependent offenders and traditional offenders (N = 508) registered by the Dutch public prosecutors' office, this study addresses two research questions. First, it will be examined which clusters of crimes can be identified empirically, by studying which self-reported crimes are often committed by the same offender and to what extent cyber-dependent offending co-occurs with traditional offending. Second, it will be examined which motivations or justifications the offenders provide for the different crime clusters and by which motivations the crime clusters can be distinguished from the others. The goal of this paper is not to identify new motivations, but to build on the motivations that have already been identified in the literature and examine to what extent these motivations are related to the different cybercrime clusters that can be identified among a known offender population.

This study thereby contributes to the literature by, first, empirically assessing assumptions about the co-occurrence of different types of cyber-dependent crime and traditional crime and comparing different clusters of cybercrime with traditional crime clusters on the motivations provided by offenders. Second, it will address an understudied population of adult offenders in the Netherlands, which will shed light on the motivations of cyber-offenders who have been in contact with the justice system in the past.

5.2 Data and methods

5.2.1 Sample and procedure

The 2000-2013 Public Prosecutor's Office's database was used to select all 1,100 suspects of cyber-dependent crimes in that period and a random sample of 1,127 traditional suspects. Suspects of cyber-dependent crime were oversampled in order to include a maximal number of this type of offences in the sample, and thus to maximise the amount of variation in measured crime types. A purely random sample would likely not have resulted in a sufficient number of cyber-offenders. It should be stressed that this procedure does not affect the results of regression and principal component analysis outcomes. It should further be noted that both cyber-dependent and traditional suspects received the same survey and were asked to self-report on both their cyber-offending and traditional offending. Thus, both groups could self-report both types of crime.

The 928 cybercrime suspects and 875 traditional suspects who had a valid mailing address and had not passed away, received an invitation letter in the summer of 2015 for participation in an online survey. The letter included a web link and unique password, information on the 50 euro incentive voucher for full participation, the scope and content of the survey, and the option to complete the survey on paper or through a Tor Hidden Service Website[3]. Further details on selection procedure, confidentiality, and a consent form were provided on the first page of the survey.

The aim was to have equal samples of cybercrime and traditional suspects, but response rates were higher in the cybercrime sample. Therefore, only traditional sample respondents received reminder letters after two and four weeks. After six weeks 268 cybercrime suspects (28.88%) and 141 traditional suspects (16.11%) had completed the full survey. To increase the number of traditional suspects in the sample, exactly the same procedure was used to invite a new random sample of 781 traditional suspects. After another six weeks 268 cybercrime suspects (28.88% response rate) and 270 traditional suspects (16.30% response rate) completed all questions relevant for this paper.

[3] Communication with this type of website is completely encrypted and less easy to trace. Three traditional sample respondents completed the survey on paper and three cybercrime sample respondents completed it through the Tor Hidden Service website.

5.2.2 Measures

Self-reported offending

Dichotomous variables were created based on self-report questions about thirteen cyber-dependent crimes and eleven traditional crimes (1 = committed the crime at least once in preceding twelve months). Cybercrime questions were based on the Dutch National Cyber Security Centre (2012) list of cyber-dependent crime and the Computer Crime Index of Rogers (2001) and included: guessing passwords, other hacking, digital theft, damaging data, defacing websites or online profiles, phishing, DoS attacks, spamming, taking control over IT-systems, intercepting communication, malware use or distribution, selling data, and selling credentials. Traditional offences were based on Svensson et al. (2013) and Dutch criminal law and included: vandalism, burglary, carrying a weapon, using a weapon, stealing, threats, violence, selling drugs, tax fraud, insurance fraud, and buying or selling stolen goods.

Motivation

For each different crime reported by a respondent, respondents were asked to indicate on a 5-point scale (totally disagree - totally agree) about nine motivations which were applicable the last time they committed that crime. These nine motivations were based on both theoretical and empirical literature and included four intrinsic motivations, four extrinsic motivations and financial motivation. Intrinsic motivations (IM) were: ‘boredom / curiosity / excitement’ (IM1), ‘fun / felt good’ (IM2), ‘challenging / educational’ (IM3), and ‘see how far I could go’ (IM4). Extrinsic motivations (EM) were: ‘damage something’ (EM1), ‘revenge / anger / to bully’ (EM2), ‘put things straight / deliver a message’ (EM3), and ‘impress others / gain power’ (EM4). Financial motivation (FM) was formulated as ‘to earn something with it’. In the analyses dichotomous variables (1 = agree) indicate if the respondent agreed or totally agreed that a motivation was applicable when committing the crime.

5.2.3 Analytical strategy

Thirty of the respondents had missing values on one or more of the offending variables (5.58%) and were excluded from the analyses. For the first research question, the remaining sample (N = 508; 77.95% male; M_{age} = 37.16 years) was used for the principal component analysis in which it was examined which clusters of crimes were present in the data. Based on the highest factor loading in the pattern matrix, each crime type was assigned to one of the crime clusters.

For the second research question, only respondents who self-reported at least one crime (N = 153) were used in the analyses on motivations. Together these respondents committed 420 different offences (on average 2.75 per offender). Coincidently exactly half of these were traditional crimes and half were cybercrimes. As offenders could indicate for each different crime which motivations were applicable, each offender-crime combination was analysed as a different observation, while correcting for intra-individual correlation by using clustered analyses. After inspecting prevalence rates of different motivations per crime cluster, multivariate probit models with each motivation were used to examine which crime clusters were statistically significantly different from each other in the extent to which the motivation played a role in committing those crimes. Estimating nine separate models for each motivation would result in stochastically dependent estimates for the different crime clusters, therefore multivariate probit models were used (for STATA, see Cappellari & Jenkins, 2003) to gain efficient parameter estimates that are not stochastically dependent.

5.3 Results

5.3.1 Offending clusters

The principal component analysis with oblique rotation indicated seven factors with an eigenvalue above one. Based on the highest factor loading in the rotated pattern matrix in Appendix A, all crimes were assigned to one of the seven crime clusters[4]. The clusters and their prevalence rates are summarised in Table 5.1 It shows that there is a distinction between cyber-offending and traditional offending, as the analyses indicated four clusters that included only cyber-dependent crimes and three clusters that included only traditional crimes. No cluster included both cybercrime and traditional crime.

The cybercrime clusters seem to be based on crimes that are functionally related as they can be part of the same modus operandi and/or crimes that require a similar environment or skill set. For example, for hacking and related crimes (C1), you first have to hack into a system to steal data from it. Similarly, before you intercept communication you need to take control over an IT-system (C3) and you can use malware to steal data and credentials that you can sell (C4). The internet related offences (χ^2) generally take place by using the internet, while the other crimes are more based on IT-systems, hence the internet related crimes share an environment and skill set. In line with Bachmann and Corzine (2010) this indicates differences between phishers, spammers, virus coders, and hackers.

[4] It should be noted that some crimes also load on another cluster, as they have another factor loading above 0.30. For clarity of the interpretation and the further analyses on motivations, the highest factor loading is used to assign each crime to only one cluster.

Table 5.1.

Prevalence rates of crime clusters and underlying offences in sample

Cybercrime		N	%[1]	Traditional crime		N	%[1]
	Guessing password	30	7.14				
	Digital theft	27	6.43		Tax fraud	35	8.33
	Hacking	24	5.71		Stolen goods	22	5.24
	Damaging data	20	4.76		Insurance fraud	15	3.57
C1:	Total hacking and related	101	24.05	T1:	Total white-collar	72	17.14
	Defacing	30	7.14				
	Phishing	15	3.57		Vandalism	19	4.52
	DoS	8	1.90		Burglary	6	1.43
	Spam	5	1.19		Using a weapon	5	1.19
C2:	Total internet related	58	13.81	T2:	Total vandalism	30	7.14
	Taking control	19	4.52				
	Intercepting communication	11	2.62		Stealing	26	6.19
C3:	Total control over IT-systems	30	7.14		Threats	24	5.71
	Malware use or distribution	11	2.62		Violence	23	5.48
	Selling data	6	1.43		Carry a weapon	20	4.76
	Selling credentials	4	0.95		Selling drugs	15	3.57
C4:	Total malware and selling	21	5.00	T3:	Total criminal life-style	108	25.71
Total number of crimes (both cybercrime and traditional crime)						420	100.00

1: percentage of total number of crimes

For traditional crime, crimes in the first cluster are white-collar crimes (T1). The second cluster mainly includes vandalism, but also burglary and using a weapon. These are the least common crimes and only three of these offenders did not commit vandalism. Hence, it is called vandalism (T2). The third cluster is a mix of crimes that often occur in a criminal life-style (T3).

5.3.2 Motivations

Each time the prevalence rates of motivations by crime cluster are discussed in the following sections, these rates can be found in Table 5.2 The documentation on the significance of differences in motivations between clusters can be found in Appendix B.

Intrinsic motivations cybercrime

In line with most literature, the prevalence rates (Table 5.2) indicate that for all cybercrime clusters intrinsic motivations are most important. ‘Boredom / curiosity / excitement’ (IM1) is the most prevalent motivation for all cybercrime clusters. ‘Challenging / educational’ (IM3) is just as often indicated as a motivation for control over IT-systems (C3). That is also an important motivation for hacking and related crimes (C1), while ‘fun / felt good’ (IM2) is the second most important motivation for internet related crimes (C2) and malware and selling (C4). The comparison models (Appendix B) show only two statistically significant differences in intrinsic motivations. First, when comparing hacking and related crimes (C1) to internet related crimes (C2) offenders more often (marginally significant) indicate ‘boredom / curiosity / excitement’ (IM1). Second, for malware and selling (C4) compared to control over IT-systems (C3) offenders more often indicate ‘fun / felt good’ (IM2).

Table 5.2.
Prevalence rates of motivations per crime cluster

	C1: hacking and related		C2: internet related		C3: control IT-systems		C4: malware and selling		T1: white-collar		T2: vandalism		T3: criminal life-style	
	N	%[1]	N	%[1]	N	%[1]	N	%[1]	N	%[1]	N	%[1]	N	%[1]
IM: Intrinsic motivations														
IM1: Boredom/curiosity/ excitement	38	37.62	13	22.41	8	26.67	8	38.10	8	11.11	6	20.00	16	14.81
IM2: Fun/felt good	13	12.87	12	20.69	3	10.00	5	23.81	16	22.22	8	26.67	17	15.74
IM3: Challenging/ educational	25	24.75	9	15.52	8	26.67	4	19.05	8	11.11	4	13.33	13	12.04
IM4: See how far I could go	16	15.84	7	12.07	5	16.67	3	14.29	10	13.89	4	13.33	13	12.04
EM: Extrinsic motivations														
EM1: Damage something	5	4.95	5	8.62	0	0.00	0	0.00	2	2.78	4	13.33	7	6.48
EM2: Revenge/anger/ to bully	7	6.93	12	20.69	1	3.33	1	4.76	4	5.56	5	16.67	29	26.85
EM3: Put things straight/ deliver message	17	16.83	12	20.69	3	10.00	0	0.00	8	11.11	6	20.00	28	25.93
EM4: Impress others/ gain power	8	7.92	4	6.90	1	3.33	1	4.76	3	4.17	3	10.00	6	5.56
FM: Financial motivation														
FM: Earn something	3	2.97	3	5.17	1	3.33	1	4.76	44	61.11	4	13.33	19	17.59

1: percentage of all crimes of this crime cluster for which the offender indicated this motivation as true. As respondents could indicate more than one type of motivation as true or all motivations as not true for each crime, these percentages do not add up to 100.

Financial motivations cybercrime

In contrast to claims in the theoretical literature, but in line with most previous empirical work, financial motivations (FM) are almost absent for all cybercrime clusters, even for malware and selling crimes (C4). Therefore, there are no statistically significant differences between cybercrime clusters on financial motivations.

Extrinsic motivations cybercrime

In line with claims in the literature, extrinsic motivations are less prevalent for cybercrime than intrinsic motivations. Nevertheless, most statistically significant differences between cybercrime clusters can be found in these extrinsic motivations. 'Damage something' (EM1) is never indicated as a motivation for control over IT-systems (C3) and malware and selling (C4), while it is indicated a few times for hacking and related crimes (C1) and internet related crimes (C2), which is a statistically significant difference. Similarly, 'put things straight / deliver a message' (EM3) was never indicated for malware and selling (C4), while it was quite often indicated for other cybercrime clusters and therefore this statistically significantly distinguished malware and selling (C4) from all other cybercrime clusters. Especially for the internet related crimes (C2) this is in line with previous research (Denning, 2011; Holt, 2009b). But, in line with Woo et al. (2004), 'revenge / anger / bully' (EM2) is just as often indicated as a motivation for internet related crimes (C2) and this statistically significantly distinguishes those crimes from hacking and related crimes (C1) and control over IT-systems (C3). In contrast to suggestions in the literature, 'impress others / gain power' (EM4) is not often indicated for any cybercrime, but for hacking and related crimes (C1) and internet related crimes (C2) this is marginally significantly more often indicated compared to control over IT-systems (C3).

Comparison cybercrime traditional crime

In contrast to claims of Grabosky (2000, 2001) and Grabosky and Walkley (2007), the results show that cybercrime does not only distinguish itself from traditional crime by challenge-related motivations, but also by other motivations. Only, the motivation 'see how far I could go' (IM4) is indicated a few times for all crime clusters, both cybercrime and traditional crime, and therefore does not differ statistically significantly between any of the clusters in the comparative models. For all other intrinsic, extrinsic and financial motives, statistically significant differences are observed between cybercrime and traditional crime.

While intrinsic motivations are relatively more common for cybercrimes, extrinsic motivations are relatively more often indicated for traditional crimes. The most important differences are observed for white-collar crimes (T1), followed by the criminal life-style crimes (T3). This supports the findings of Turgeman-Goldschmidt (2011) that hackers cannot be compared to white-collar offenders. For white-collar crimes (T1) the financial motivation (FM) is by far the most important and it is statistically significantly more common compared to all other crime clusters, both cybercrime and traditional crime. In addition, compared to the cybercrimes the financial motivation (FM) is also more common for the other traditional crime clusters, but this difference is only statistically significant for criminal life-style crimes (T3) compared to hacking and related (C1), internet related (C2) and control over IT-systems (C3) crimes.

For intrinsic motivations, most differences can be found for the motivation 'boredom / curiosity / excitement' (IM1) that is much more common for the cybercrime clusters, especially compared to the white-collar crimes (T1) and to a lesser extent compared to the criminal life-style crimes (T3). The difference is only once marginally significant for vandalism (T2) compared to hacking and related crimes (C1). But for white-collar crimes (T1) it is a statistically significant or marginally significant difference compared to all cybercrime clusters. For criminal life-style crimes (T3) it is statistically significant compared to hacking and related crimes (C1) and malware and selling (C4).

Additionally, as claimed by Grabosky (2000, 2001) and Grabosky and Walkley (2007) 'challenging / educational' (IM3) is a common motivation for hacking and related crimes (C1) and control over IT-systems (C3), while it is not common for traditional crime. This difference is statistically significant for hacking and related crimes (C1) compared to white-collar crimes (T1), and criminal life-style crimes (T3) and marginally significant for white-collar crimes (T1) compared to control over IT-systems (C3). Interestingly, similar to internet related crimes (C2) and malware and selling (C4) 'fun / felt good' (IM2) is quite common for white-collar crimes (T1) and vandalism (T2). However, it is not common for control over IT-systems (C3), hence this difference is statistically significant for white-collar crimes (T1) and marginally significant for vandalism (T2). This is the only difference between cybercrime and vandalism (T2) for intrinsic motivations.

For extrinsic motivations, 'put things straight / deliver a message' (EM3) was never indicated for malware and selling (C4) and rarely for control over IT-systems (C3). As this is an important motive for vandalism (T2) and criminal life-style crimes

(T3), and to a lesser extent for white-collar crimes (T1), this difference is statistically significant between malware and selling (C4) and all traditional clusters and marginally significant between criminal life-style crimes (T3) and control over IT-systems (C3). Similarly, 'damage something' (EM1) is never indicated for C3 and C4, and although it is also not very common for traditional crimes, it is still statistically significantly more common for all traditional crimes compared to C3 and C4. Interestingly, 'damage something (EM1) is statistically significantly more often a motive for vandalism (T2) compared to hacking and related crimes (C1), while it is less often a motive for white-collar crimes compared to internet related crimes (C2).

'Revenge / anger / bully' (EM2) is a quite common motivation for vandalism (T2) and very common for criminal life-style crimes (T3). As it is only a quite common motivation for internet related crimes (C2) while almost absent for the other cybercrimes, it differs statistically significantly between the criminal life-style crimes (T3) and the other tree cybercrime clusters (C1, C3, C4). Additionally, as it is very uncommon for control over IT-systems (C3) it is statistically significantly different between C3 and vandalism (T2). In contrast, as it is an important motivation for internet related crimes (C2) and almost absent for white-collar crimes (T1), this difference is also statistically significant. Lastly, 'Impress others, gain power' is not very common for all crimes, but marginally significantly more common for vandalism (T2) and criminal life-style crimes (T3) compared to control over IT-systems (C3) and malware and selling (C4).

Comparison motivations between traditional crimes

As this paper focusses on cybercrime in comparison to traditional crime, results for traditional crimes will be discussed briefly, but documentation on all statistically significant differences can be found in Appendix B. While the different cybercrime clusters are mostly committed out of intrinsic motivations and show differences based on extrinsic motivations, there is a lot more variation in motivations between the traditional crime clusters. White-collar crimes (T1) have a mostly financial motivation, while vandalism (T2) and criminal life-style crimes (T3) show a somewhat mixed picture. Even though the prevalence rates show that intrinsic motivations are more common for vandalism (T2), while extrinsic motivations are more common for criminal life-style crimes (T3), there is no statistically significant difference between the motivations of these two traditional crime clusters.

Only the white-collar crimes (T1) show statistically significant differences with the other two crime clusters, but only in financial and extrinsic motivations. The most important difference is that financial motivations are much more common, but some extrinsic motivations are less common for white-collar crimes (T1) compared to the other two. ‘Damage something’ (EM1) and ‘revenge / anger / bully’ (EM2) are statistically significantly or marginally significantly more common for the other traditional crimes (T2 and T3). In addition, ‘put things straight / deliver a message’ (EM3) is very common for criminal life-style crimes (T3) and therefore statistically significantly distinguishes those from the white-collar crimes. Lastly, ‘impress others / gain power’ (EM4) is not very common for all traditional crime clusters and therefore shows no statistically significant differences.

5.4 Conclusion and discussion

In this paper some gaps in the literature on cybercrime have been addressed, by using self-report data from the understudied population of adult cyber-offenders and traditional offenders registered by the Dutch public prosecutors’ office. First, it was examined to what extent cyber-dependent offenders can be distinguished from traditional offenders, by analysing which clusters of cyber-offences and traditional offences are often committed by the same offender. Second, using these clusters it was explored which motivations the offenders provided for committing those crimes and to what extent these clusters can be distinguished from the others by these motivations.

With regard to the first objective, it was found that cyber-dependent crimes form a distinct group of offences that rarely co-occur with traditional crimes. This is in line with the hypothetical distinction between traditional crimes and cyber-dependent crimes. The hypothetical assumption in theoretical literature, that cyber-dependent crimes could be part of the same modus-operandi as traditional crimes, could not be verified with this data, but three out of the four cybercrime clusters appeared to be crimes that are part of the same cyber-modus operandi. These three clusters were hacking and related crimes, control over IT-systems and malware and selling crimes. The internet related crimes were more likely clustered together because they require the same skills set, as, unlike the others, they mainly take place on the internet instead of on specific IT-systems. To some extent this is in line with hypothetically distinguished cyber-dependent crime clusters as described in the theoretical literature (Bachmann & Corzine, 2010; McGuire & Dowling, 2013).

With regard to the second objective, it was found that intrinsic motivations were most important for all cybercrime clusters. This is in line with the empirical literature. Additionally, the comparative analyses showed that although there is some variation in the relative importance of different intrinsic motivations for the different cybercrime clusters, these can hardly be used to differentiate between the different cybercrime clusters. In contrast to suggestions in the theoretical literature, however, very little offenders indicated they committed their cybercrimes for financial gain, even for crimes where they sold data or credentials. Offenders indicated that these are still mostly committed out of boredom, curiosity or excitement or other intrinsic motivations. Thus these offenders, who have been in contact with the police earlier in their offending career, have not shifted to offending for financial gain. This is in contrast to some literature that suggests that later in their career offenders shift to financial motivations (Bachmann, 2011; Bachmann & Corzine, 2010; Xu et al., 2013).

While the intrinsic motivations seem to indicate that internet related crimes are more comparable to malware and selling crimes, the extrinsic motivations actually distinguish control over IT-systems and malware and selling from hacking and related crimes and internet related crimes. While offenders of the latter crimes quite often indicate extrinsic motivations for these crimes, especially for internet related crimes, they virtually never indicate such motivations for control over IT-systems or malware and selling. Additionally, the internet related crimes seem to be distinguished from all other cybercrime clusters as they are most often committed out of extrinsic motivations, especially out of revenge anger or to bully someone. In line with arguments of Leukfeldt et al. (2013) these may be crimes that are easier to commit and therefore more general motivations, like revenge, are more important. In addition, most of these crimes are more visible to others than the other cybercrimes and can potentially be committed on a large scale, which increases their usefulness for extrinsically motivated offending.

In contrast to empirical evidence based on forums, in this offender sample the cybercrimes were generally not committed initially to impress others or gain power. At the moment a cybercrime is committed, there may generally be no one around to show off to. Some offenders may brag about it online afterwards, but apparently most of them do not start committing the crime for status. As discussed by Jordan and Taylor (1998) the status and rewards received from online friends may stimulate future offending, but may not provide an initial motivation for offending. This could reduce the usefulness of prevention strategies that are based on the assumption that offenders will stop committing crimes if it does not result in more status.

The comparisons between cybercrime and traditional crime showed a lot of differences in motivations between cybercrime and traditional crime clusters. Most importantly, as financial motivations are almost absent for all cybercrimes, this distinguishes them from the white-collar crimes, which is in line with Turgeman-Goldschmidt (2011). Additionally, that is also an important difference between the cybercrimes and criminal life-style crimes, but criminal life-style crimes can also be distinguished from cybercrimes by showing more extrinsic motivations. It should be noted, however, that internet related crimes, and to a lesser extent hacking and related crimes, are more similar to traditional crimes in their motivations, especially in their extrinsic motivations, than control over IT-systems and malware and selling crimes. This may indicate that the latter crimes are more specialised and technical in nature, which potentially results in more distinctly different offenders and motivations.

With respect to intrinsic motivations, cybercrimes can be distinguished from traditional crimes, especially as they are largely committed out of boredom, curiosity or excitement or because it is challenging or educational. It should be noted, however, that vandalism is quite similar to cybercrimes in intrinsic motivations. Nevertheless, when looking at extrinsic motivations, there are a lot of differences between the cybercrimes and vandalism. Therefore the results cannot completely verify the hypothetical claim of Kirwan and Power (2013) that cybercrime, specifically malware use, is similar to vandalism and therefore has similar motivations.

These results provide useful information for both investigation and prevention. First, these results could be used after a cybercrime has occurred, to assess the possible chain of crimes that were committed and the underlying motivations of the offender, based on empirical data instead of only hypothetical assumptions. Second, as motivations for cybercrime are not similar to traditional crimes and more intrinsic, this offers new opportunities for crime prevention that may not have been very useful for traditional crimes. For example, if offenders who have been in contact with the police still mainly commit their crimes out of boredom, curiosity or excitement, or for the challenge or educational aspect, helping convicts to find legal daily activities that can satisfy these needs may be more useful to prevent re-offending for cybercrime than for traditional crime. The skills needed to commit these cybercrimes are actually skills that can be used in legitimate daily activities.

Even though the results and implications address an important gap in the literature on cybercrime, the sample and method also have their limitations. First of all, like most research on crime and criminals, there is a dark number and the sample could be selective. The sample is based on respondents who have been in contact with the police in the past. This high risk sample was necessary to find two comparable groups of cybercrime and traditional offenders and find a sufficient number of cyber-dependent offenders, who are less prevalent in the general population than cyber-enabled offenders. Nevertheless, when using these results, it should be kept in mind that these are the clusters of crimes and related motivations that are reported by offenders who have been in contact with the police and have subsequently continued committing crime. Therefore, these clusters and related motivations may be different among first offenders or offenders who are able to avoid the long arm of the police.

As discussed in the introduction an important limitation of asking offenders about their motivations after they committed a crime, is that it may only show their justifications for offending, instead of the actual motivation at the moment they were committing the crime. In addition, offenders may choose to report a more socially accepted motivation as curiosity or challenge and not report their financial motivation, for example. However, the prevalence rates of reported financial motivations were very high for white-collar crimes, which may indicate that respondents did not feel the urge to only report socially accepted motivations in this study.

Even though it is challenging to study motivations for committing crimes, it is important to examine those motivations as they may guide us to possible prevention methods as discussed above. Most criminological research on both cybercrime and traditional crime just assumes the existence of motivated offenders and research on cybercrime assumes that motivations for cybercrime are similar to motivations for traditional crime. The analyses in this paper have empirically shown the large differences that exist between cybercrime and traditional crime clusters.

5.5 Appendix A: Pattern matrix principal component analysis

	Factor						
	1	2	3	4	5	6	7
	(α=0.75)	(α=0.62)	(α=0.60)	(α=0.74)	(α=0.63)	(α=0.66)	(α=0.59)
	Cybercrime factor C1	Traditional crime factor T1	Cybercrime factor C2	Cybercrime factor C3	Traditional crime factor T2	Traditional crime factor T3	Cybercrime factor C4
Guessing password	**0.70**	0.03	-0.08	0.10	0.08	-0.09	0.07
Digital theft	**0.77**	-0.10	0.14	-0.03	-0.11	0.07	0.05
Hacking	**0.65**	0.18	-0.13	0.35	-0.18	-0.06	0.06
Damaging data	**0.65**	0.05	0.07	0.10	0.12	0.03	-0.09
Tax fraud	0.00	**0.77**	0.09	0.09	-0.27	0.06	-0.02
Stolen goods	0.07	**0.63**	-0.02	-0.06	0.22	0.09	-0.03
Insurance fraud	-0.01	**0.71**	0.12	-0.03	0.11	-0.14	0.08
Defacing	-0.07	0.11	**0.47**	0.14	-0.21	0.34	0.11
Phishing	0.38	-0.07	**0.50**	-0.07	0.04	0.17	0.19
DoS	-0.04	0.16	**0.61**	0.26	0.12	-0.02	0.03
Spam	0.08	0.13	**0.78**	-0.08	0.09	-0.21	0.00
Taking control	0.19	-0.01	0.03	**0.83**	0.03	0.08	-0.07
Intercepting communication	0.21	0.01	-0.04	**0.66**	0.34	-0.11	0.00
Vandalism	0.09	0.14	0.29	0.07	**0.37**	0.26	-0.23
Burglary	-0.06	0.20	0.22	0.25	**0.63**	-0.12	0.09
Using weapon	0.04	0.02	0.02	0.12	**0.71**	0.18	0.19
Stealing	0.35	0.25	0.14	-0.08	0.05	**0.40**	-0.14
Threats	-0.01	-0.05	0.02	0.07	-0.10	**0.75**	0.11
Violence	-0.01	0.12	-0.15	-0.10	0.35	**0.54**	0.28
Carry weapon	0.10	-0.17	0.20	0.00	0.25	**0.50**	-0.26
Selling drugs	-0.04	0.35	-0.24	0.05	0.08	**0.54**	-0.06
Malware	-0.14	-0.02	0.14	0.48	-0.11	0.15	**0.55**
Selling data	0.43	0.01	-0.04	-0.11	0.04	-0.08	**0.64**
Selling credentials	-0.01	0.05	0.18	0.03	0.27	0.09	**0.70**

Note: pattern matrix with oblique rotation, results with varimax rotation indicated the same classification of crimes (results available upon request)

5.6 Appendix B: Evidence for significant differences in motivations between clusters

These tables are based on clustered (respondent-crime) multivariate probit models. The underlying parameter estimates are available upon request.

Dark grey areas show comparisons between a specific cybercrime and a specific traditional crime cluster, while light grey areas show comparisons between a specific cybercrime and another cybercrime cluster, or a specific traditional crime and another traditional crime cluster.

+ indicates more common for crime cluster in left column compared to crime cluster in upper row

– indicates less common for crime cluster in left column compared to crime cluster in upper row

+++/– – – p < .001; ++/– – p < .01; +/– p < .05; (+)/(–) p < .10 (two-tailed)

IM: Intrinsic motivations

IM1: Boredom/curiosity/excitement

	C1	C2	C3	C4	T1	T2	T3
C1		(+)			+++	(+)	+++
C2	(–)				(+)		
C3					(+)		
C4					++		+
T1	– – –	(–)	(–)	– –			
T2	(–)						
T3	– – –			–			

IM3: Challenging/educational

	C1	C2	C3	C4	T1	T2	T3
C1					+		+
C2							
C3					(+)		
C4							
T1	–		(–)				
T2							
T3	–						

IM2: Fun/felt good

	C1	C2	C3	C4	T1	T2	T3
C1							
C2							
C3				–	–	(–)	
C4			+				
T1			+				
T2			(+)				
T3							

IM4: See how far I could go

	C1	C2	C3	C4	T1	T2	T3
C1							
C2							
C3							
C4							
T1							
T2							
T3							

EM: Extrinsic motivations

EM1: Damage something

	C1	C2	C3	C4	T1	T2	T3
C1			+++	+++		–	
C2			+++	+++	+		
C3	– – –	– – –			– – –	– – –	– – –
C4	– – –	– – –			– – –	– – –	– – –
T1		–	+++	+++		–	(–)
T2	+		+++	+++	+		
T3			+++	+++	(+)		

EM3: Put things straight/deliver a message

	C1	C2	C3	C4	T1	T2	T3
C1				+++			
C2				+++			
C3				+++			(–)
C4	– – –	– – –	– – –		– – –	– – –	– – –
T1				+++			–
T2				+++			
T3			(+)	+++	+		

EM2: Revenge/anger/to bully

	C1	C2	C3	C4	T1	T2	T3
C1		–					– –
C2	+		++		+		
C3		– –				– –	– –
C4							–
T1		–				(–)	– –
T2			++		(+)		
T3	++		++	+	++		

EM4: Impress others/gain power

	C1	C2	C3	C4	T1	T2	T3
C1			(+)				
C2			(+)				
C3	(–)	(–)				(–)	(–)
C4							
T1							
T2			(+)				
T3			(+)				

FM: Financial motivation

FM: Earn something

	C1	C2	C3	C4	T1	T2	T3
C1					– – –		–
C2					– – –		– –
C3					– – –		–
C4					– – –		
T1	+++	+++	+++	+++		+++	+++
T2					– – –		
T3	+	++	+		– – –		

Chapter 6

General conclusion and discussion

6.1 Introduction

The rise in criminal opportunities by using IT-systems and the unique nature of cyber-dependent crime, resulted in the need to gain insight into the extent to which the people who commit these crimes are similar to or different from traditional offenders. Therefore, the main goal of this dissertation was to empirically compare cyber-offenders with traditional offenders on four important domains in criminology: offending over the life-course, personal and situational risk factors for offending and victimisation, similarity in deviance in the social network, and motivations related to different offence clusters. Previous research had already identified several correlates of cyber-offending that are similar to correlates of traditional offending, but empirical comparisons of the strength of these correlates were non-existent. In addition, non-US adult samples and cyber-dependent crimes that require advanced IT-skills were understudied. Therefore, this dissertation contributed to the literature by comparing cyber-dependent offending with traditional offending among Dutch adults.

6.2 General results

The following sections will first briefly summarise the most important results of each empirical chapter. This will provide the answers to the question to what extent cyber-offenders differ from traditional offenders in each of these four domains. Subsequently, the results will be interpreted in a general conclusion.

6.2.1 Longitudinal life-course study (Chapter 2)

In Chapter 2, a longitudinal dataset of registration data for the period 2000-2012 was used to study cyber-offending and traditional offending over the life-course. Based on the nature of cyber-offending it was argued that the life circumstances that generally reduce the likelihood of traditional offending, may not be equally influential for cyber-offending. For personal life circumstances it was found that living with a partner or with a partner and a child reduces the likelihood of cyber-offending, and living as a single parent increases the likelihood of offending. In contrast to expectations, these estimates were in the same direction and even stronger for cybercrime compared to traditional crime.

With respect to professional life circumstances, the results were more in line with the expectations. There was no statistically significant effect of employment or enrolment in education on cyber-offending, while these life circumstances did reduce traditional offending statistically significantly. Within the complete offender population of this study, the results even pointed to some interesting differences between general employment and employment in the IT-sector and enrolment in education. In line with the estimates for traditional crime, general employment reduced the likelihood of cyber-offending. In contrast, employment in the IT-sector increased the likelihood of cyber-offending. Similarly, being enrolled in education, both general- and IT-education, also increased the likelihood of cyber-offending. These results regarding personal and professional life circumstances seem to indicate that, even though cyber-offending is less visible than traditional offending, social control of others can reduce the likelihood of cyber-offending. However, some traditionally protective life circumstances can increase opportunities for cyber-offending and apparently the control of others in these situations cannot prevent a person from using those opportunities to commit cybercrime.

6.2.2 Correlates of offending, victimisation, and victimisation-offending (Chapter 3)

Based on the cross-sectional dataset collected for this dissertation, this chapter studied risk factors for victimisation and offending for cybercrime and traditional crime. From the literature, there appeared to be an overlap of cybercrime offending and victimisation, just as for traditional crime. Therefore, this study compared patterns in personal and situational risk factors for separate groups of offenders-only, victims-only and victim-offenders, between cybercrime and traditional crime. In line with the literature, the results showed that physical convergence of victims and offenders is not necessary for a victim-offender overlap to occur, as the data also indicated the existence of a victim-offender overlap for cyber-dependent crime.

For cybercrime, offenders-only committed the relatively more technically sophisticated crimes compared to victim-offenders. This was also reflected in the risk factors for offenders-only, as the likelihood of offending-only was higher if a person had more IT-skills, did not have a statistically significantly low self-control, and had online activities in which they could increase their criminal IT-skills. These offenders-only appear to be capable of committing the more sophisticated types of cybercrime and simultaneously reduce their risk for victimisation. For victim-offenders, on the other hand, IT-skills also increased the likelihood of victimisation-offending, but less so compared to offenders-only. In addition, low self-control increased the likelihood of victimisation-offending. Lastly, more general online routine activities, in which both opportunities for offending and risks for victimisation could emerge, were related to victimisation-offending.

When comparing these results to traditional crime, it was shown that for both types of crime, victim-offenders have more risk factors and the effect of low self-control is very similar. Differences are mostly found in situational risk factors, as the differences seem to be the result of the different context in which these crimes take place. Online activities are more important for cybercrime, while offline activities are more important for traditional crime.

6.2.3 Similarity in deviance of social network members (Chapter 4)

Based on ego-centred network data from the cross-sectional survey dataset collected for this dissertation, this chapter tested to what extent the relation between deviance of an individual and deviance of a social network member is weaker for cybercrime compared to traditional crime. First of all, in line with previous research on cybercrime, a statistically significant similarity in deviance was found. Even when controlling for the possibility that this similarity was caused by other factors, like similarity in gender or age. Nevertheless, the comparison with traditional crime indicated an important difference in the strength of the similarity in deviant behaviour, which appeared to be weaker for cybercrime.

Subsequently, this chapter explored differences between social network members. This indicated that both for cybercrime and traditional crime the relation is stronger for daily-contacted network members of the same gender. However, when comparing the differences between network members who are younger, older, or of the same age, the results indicated important differences. For cybercrime the relation is strongest for older social network members, followed by younger and same-aged contacts, while for traditional crime the relation is strongest for same-aged contacts, followed by younger and older contacts. This indicates that older role models may be relatively more important for cybercrime compared to traditional crime.

6.2.4 Clusters of offences and related motivations (Chapter 5)

This chapter used the self-reported offending questions from the cross-sectional dataset, to examine which clusters of crime could be identified in the data and to what extent cyber-dependent offenders could be distinguished from traditional offenders. In addition, the data on self-reported motivations were used to examine which motivations offenders provide for the different clusters of offending and to what extent the clusters distinguish themselves from the others by these motivations.

First of all, with regard to the clusters, the analyses indicated that cyber-dependent crime is seldom committed by offenders who also commit traditional crimes. None of the clusters that were identified included both cybercrimes and traditional crimes. The cybercrimes that were often committed by the same offender appeared to be part of the same modus operandi or to be related because they require the same skill set and context.

In contrast to most hypothetical claims in the literature on cybercrime and in contrast to traditional crimes, the cyber-offenders in this sample almost never indicated a financial motivation. In line with most empirical literature on cybercrime, but in contrast to most traditional crimes, intrinsic motivations were most important for all cybercrime clusters. Extrinsic motivations were less important for cybercrime compared to traditional crime. However, some differences between the cybercrimes could be observed for extrinsic motivations, as hacking and internet related crimes were more often committed to put things straight or to deliver a message, and the internet related crimes were also more often committed out of revenge, anger or to bully someone. In contrast to what has been reported in some literature on cybercrime, impressing others or trying to gain power was rarely indicated as a motivation for cyber-offending.

6.2.5 General conclusion

Based on the empirical research conducted on the four domains in this dissertation, the question to what extent cyber-offenders differ from traditional offenders can be answered as follows: Correlates of cyber-offending are to some extent similar to correlates of traditional offending. Nevertheless, important differences occur in each domain, which seems to be the result of the different context in which cybercrime takes place. These differences should be kept in mind when applying explanations for traditional offending to cyber-offending. Therefore, I will highlight the most important differences and connect the differences found in each domain to the differences found in the other domains.

Offenders who commit cyber-dependent crimes rarely also commit traditional crimes. This indicates that they are a specific type of offender. The context in which these offenders commit their crimes also requires them to have IT-skills, as IT-skills are an important predictor of cyber-offending. These skills seem to be learned in a different way than the skills needed for traditional offending. In relation to that, low self-control is only a risk factor for victim-offenders, who generally commit the less sophisticated types of crime. The more technical types of crime are committed by offenders-only who seem to have the ability to learn IT-skills and carefully plan and execute their crimes. Similarly, intrinsic motivations, like curiosity and the educational aspect of learning IT-skills through offending, distinguish cyber-offending from traditional offending.

Just as for traditional offending, having strong social relationships like a romantic partner and a child decreases the likelihood of cyber-offending. Nevertheless, the deviance of strong social contacts seems to be less important for cybercrime compared to traditional crime. One of the explanations for this could be the finding that impressing others is generally not a motivation for committing a cybercrime. Lastly, it is clear that opportunities for cyber-offending emerge in different situations than opportunities for traditional offending. The digital context in which these crimes are committed has changed the activities that provide opportunities and risks. This context may further increase the likelihood of offending, because of the limited perceived real-life consequences of deviant behaviour in this context and the invisibility of that behaviour.

Even though these are important differences, various correlates of cyber-offending have shown to be similar to correlates of traditional offending. Therefore, these differences do not require us to develop completely new explanations for cyber-offending. However, we also cannot simply apply explanations for traditional offenses to cyber-offenses, without taking the different context in which these crimes take place into account. As cybercrime is becoming more prevalent, it is to be expected that criminological studies will start to include these types of crime. For that purpose, it should be noted that even though some traditional explanations for offending seem to be quite robust for these new crimes, some of the predictors for traditional offending are not found for cyber-offending. This does not mean that these explanations should not be used, or that studies cannot include cybercrimes in addition to traditional crimes, but it does mean that predictions and measures based on these explanations should be adjusted to the digital domain. We should also be careful in using these traditional predictors for explaining cybercrime, without empirically testing if the evidence is just as strong for cybercrime as it is for traditional crime.

6.3 General limitations

Each empirical chapter discussed the limitations that were related to the data and measures for that specific domain. Nevertheless, some general limitations should be addressed here. First of all, the samples in this dissertation were drawn from police and prosecutor's data. For the longitudinal dataset of Chapter 2, this means that the outcome variable reflects when a person was a suspect of a crime, but it is unknown if this person was actually guilty of committing that crime and it is unknown to what extent this person also committed crimes in the years he or she was not caught by the police. For Chapter 3 to 5, this means that the population that was studied is a high risk population. The analyses indicated which present-day risk factors, social contacts and motivations were related to present-day self-reported offending of people who had been caught by the police for committing a crime in the past, prior to the twelve-month period of the self-report questions.

Like most research on crime and criminals, there is a dark number and therefore using police or prosecutor's data could also result in a selective sample, as it only reflects the people who have been caught for committing a crime. This means that the results may be different in general population samples and among offenders who have been able to avoid the long arm of the police. For example, if offenders with financial motivations are better able to avoid apprehension than offenders with intrinsic motivations, then the results do not reflect the relative importance of different motivations for all cyber-offenders. For cybercrime, it is well known that apprehension rates are very low (e.g., Leukfeldt et al., 2013) and probably much lower than for traditional crime. This may have resulted in a more selective sample of cyber-offenders compared to traditional offenders. On the other hand, response rates among cybercrime suspects where almost twice as high compared to traditional suspects. This could mean that the sample of traditional suspects who actually responded is more selective than the sample of cybercrime suspects who responded. Nevertheless, studying cyber-dependent offending requires the use of high risk samples as it is not very common in the general population. For comparing these crimes with traditional crimes, these samples drawn from police and prosecutor's data provided the best way to gain relatively comparable samples of offenders.

Secondly, for Chapter 2 the nature of the data limited the depth of the variables under study. For example, registration data cannot inform us about the strength of social bonds and people's actual daily activities. Therefore, it remains unknown which specific aspects of the life circumstances that were studied were related to an increase or decrease in the likelihood of offending. The data used in Chapter 3 to 5 provided more in-depth measures, but the cross-sectional nature of the data limited the ability to draw strong causal conclusions from the analyses. For example, it is unknown to what extent offending has a causal relationship with victimisation and it is unknown to what extent the similarity in deviance between social network members is the result of selection or influence processes.

Third, the data used are based on Dutch adults. This is both an advantage and a limitation. Research on cyber-offending among adults in populations outside of the US is rare. Nevertheless, it is unknown to what extent the results on adults also apply to juveniles and adolescents, while for both cybercrime and traditional crime juveniles and adolescents are more likely to commit crimes than adults. In addition, it is also unknown to what extent the results on Dutch offenders also apply to offenders from other countries. For example, Dutch cyber-offenders may be less skilled than cyber-offenders from other countries (e.g., Chua & Holt, 2016; European Cybercrime Center, 2014; Holt & Kilger, 2012). In addition, cybercrimes can be easily committed across jurisdictions and offenders who commit their crimes across jurisdictions are generally less easy to identify (Brenner, 2006; Jaishankar, 2009; Kshetri, 2013; Leukfeldt et al., 2013). This means that it is likely that Dutch offenders who commit their crimes within the Dutch jurisdiction, were overrepresented in the data used in this dissertation.

Lastly, this dissertation empirically compared a specific group of cyber-dependent offenders to a general and quite diverse group of traditional offenders. The question could be raised if it would have been more helpful to compare cyber-offenders with a specific type of traditional offender. For example, a type of offender that is expected to be more similar to cyber-offenders. There was, however, no empirical indication for selecting a specific type of traditional crime. The literature only contained some hypothetical claims that cyber-offending would, for example, be more similar to white-collar offending or property offending, or that malware use would be similar to vandalism. Chapter 5, however, questions these claims. This indicates that selecting a comparative sample of a specific type of traditional offenders, based on hypothetical claims, would not have been a better solution. In addition, there are general patterns in offending over the life-course, risk factors, and similarity in deviance of social network members that basically apply to all types of traditional offending. Apart from this dissertation, there is no empirical knowledge on the similarity of cyber-offending and traditional offending. Therefore, this overall comparison of general patterns for offending addressed the most important gap in the literature.

6.4 Future research

Each chapter already discussed some future research directions for the specific domain addressed in that chapter. However, several general directions are important to discuss here. First of all, to address the general limitations discussed above, replication in future research in different and larger samples, preferably with in-depth longitudinal data, is necessary. Different samples may include non-Dutch, general population, or high risk samples of juveniles or adolescents. To enhance the generalisability of research based on police data samples, it could also be informative to study the differences between cyber-offenders who have been caught and cyber-offenders who have been able to avoid apprehension. This could, for example, shed light on the question to what extent they differ in their motivations to commit cybercrimes.

Second, this dissertation indicated that strong social contacts show less similarity in deviant behaviour for cybercrime compared to traditional crime. This may mean that selection and influence processes that lead to similarity in deviance of social network members, do not take place to the same extent for cybercrime as they take place for traditional crime. It could, however, also mean that other, less strong, and maybe only online social network members now take the role that strong social contacts take in traditional crime. However, in contrast to this assumption, the offenders generally indicated that they did not commit the crimes to impress others or gain power. Therefore, as discussed in the The Human Factor in Cybercrime and Cybersecurity Research Agenda (Weulen Kranenbarg et al., 2017), future research could further examine to what extent selection and influence processes can be found in, for example, online forums and gaming communities. This will inform us about the usefulness of intervening in these online communities. In addition, that research could shed light on the extent to which these online social contacts and online interactions are comparable to traditional social contacts and offline interactions. This will tell us to what extent traditional offline processes that are related to offending may be adjustable to new situations in the online world.

Third, in addition to utilizing the unique nature of cybercrime to study online criminal behaviour in new ways (like analyzing forums and other digital information, see for example Holt, Smirnova, & Chua, 2016), future research on cybercrime could also learn from criminological methodologies that proved to be useful for studying traditional crime. As Rogers (2011) states: *'We need to move beyond mere anecdotes and cultural myths and adopt a scientific approach toward understanding cybercrimes and cybercriminals.* [...] *We need to apply the same scientific rigor to computer criminals that we have applied in our attempts to understand general criminal behaviours.'* (p. 234). For example, I believe that in-depth longitudinal research is necessary to (1) find the exact causal processes and life circumstances that lead to committing cybercrime or desistence from committing cybercrime, (2) identify processes of selection and influence in online and offline social networks for cybercrime, and

(3) to examine a possibly causal relationship between offending and victimisation (Weulen Kranenbarg et al., 2017). Nevertheless, as discussed in the general conclusion, it is important that studies that use traditional methodology to explain cybercrime, adjust their predictors and measures to the digital domain.

Fourth, another method that could be adopted from research on traditional crime is the use of a social network method as the one used in Weerman and Smeenk (2005), in which all network members report on their own deviant behaviour, preferably in a longitudinal design (Weulen Kranenbarg et al., 2017). If that type of study includes both cyber-offending and traditional offending for all people in a social network, this will enhance our knowledge on (1) selection and influence processes, (2) the discrepancy between perceived and actual cyber-deviance of social contacts, (3) the extent to which actual and perceived deviance of social contacts differently influences cyber-offending, and (4) to what extent the invisibility of cyber-deviance results in a larger discrepancy for cybercrime compared to traditional crime. It should, however, also be noted that general school classes that are usually used for this type of research, may not be useful for studying more technically advanced types of cyber-dependent offending, as these crimes may not be prevalent enough in these samples. Specialised primary or secondary school classes that specifically focus on students with IT-talent or other IT-related education, may be more useful.

Fifth, in addition to traditional quantitative research methods, in-depth qualitative interviews could provide us with more detailed information on what strategy offenders use if they commit a cybercrime and if they actively seek opportunities for cyber-offending or if they simply come across these opportunities by chance during their daily activities (Weulen Kranenbarg et al., 2017). In addition, these qualitative interviews may, for example, be used to shed light on the question why the similarity in deviance of strong social network members is strongest for older social network members. This may inform us if and how older mentors could be used in intervention and prevention strategies.

Sixth, as it has consistently been shown that IT-skills are related to cyber-dependent offending, future research could focus on the role of IT-skills in committing cybercrimes. It is important to study differences in the level of IT-skills needed to commit different types of cyber-dependent crime. In addition, longitudinal research could examine how people acquire IT-skills and knowledge on how to use those skills in an illegal manner over time. Furthermore, as IT-skills are very useful in legitimate daily activities, research could start developing and evaluating methods that could stimulate people to use their IT-skills in a responsible manner (Weulen Kranenbarg et al., 2017).

Lastly, this dissertation hast shown that it is not enough to simply apply traditional explanations for offending to cyber-offending. For cybercrime, in order to be able to use interventions that are based on explanations for traditional crime, it is necessary to study the differences between cyber-offenders and traditional offenders. This dissertation is therefore a first step in assessing the usefulness of the large volume of criminological literature on traditional crime. Future research could further examine other domains in the criminological literature. In addition, the context in which cybercrime takes place provides new and unique opportunities of studying criminal behaviour. In one way or another, online behaviour is registered and could therefore be used to observe criminal behaviour in ways that have not been possible with offline behaviour. However, in order to generalise results based on online behaviour to criminal behaviour in general, comparisons between online and offline criminal behaviour are necessary as well.

6.5 Practical implications

Based on the results for each domain, the individual chapters already discussed some practical implications. However, some more general implications derived from this dissertation and the existing literature are important to discuss here. It should be noted, that none of the prevention and intervention strategies discussed below have been evaluated empirically for cybercrime. In addition, the recommendations are based on a limited number of empirical studies. Therefore, authorities that are responsible for designing and executing prevention and intervention programs, are advised to carefully design and implement evaluation studies of the programs they design for cybercrime.

When using interventions designed for traditional offenders, empirically identified differences and similarities between cyber-offenders and traditional offenders should be kept in mind. It is not advisable to base the application of traditional interventions to cybercrime purely on hypothetical similarities. For example, this dissertation indicated that, in contrast to hypotheses in the literature, cyber-offenders differ from white-collar offenders with respect to their motivations for committing crimes. While financial motivations are by far the most important motivation for white collar crimes, these motivations are almost absent for cyber-offences in this sample. Therefore, interventions for cybercrime may not benefit much from reducing the expected financial gain of committing cybercrimes. In contrast to traditional crime, but in line with previous cybercrime research, this dissertation has shown that the level of IT-skills is an important predictor of cyber-offending, both when measured subjectively or with an objective IT-skills test. Cyber-offenders even indicated that they mainly commit their crimes out of curiosity and for the educational aspect of enhancing their IT-skills. Therefore, interventions may benefit from stimulating them to satisfy these needs in legitimate ways, as this may reduce their need for using and enhancing their skills in an illegal way.

Fortunately, the skills needed to commit cybercrimes are also very useful in legitimate daily activities, for example in the cybersecurity industry. One way of helping cyber-offenders to use their skills in a legitimate way may be to help them find employment in which they could use their skills. It is, however, important to note that, in contrast to traditional crime, this dissertation indicated that employment and especially employment in the IT-sector also seems to provide opportunities for committing cybercrime. Simply providing employment may, therefore, have an undesirable effect. Consequently, it is important that cyber-offenders are offered ethical guidance in their path to a legitimate profession and it is important to establish both strong formal and informal social control in their professional life.

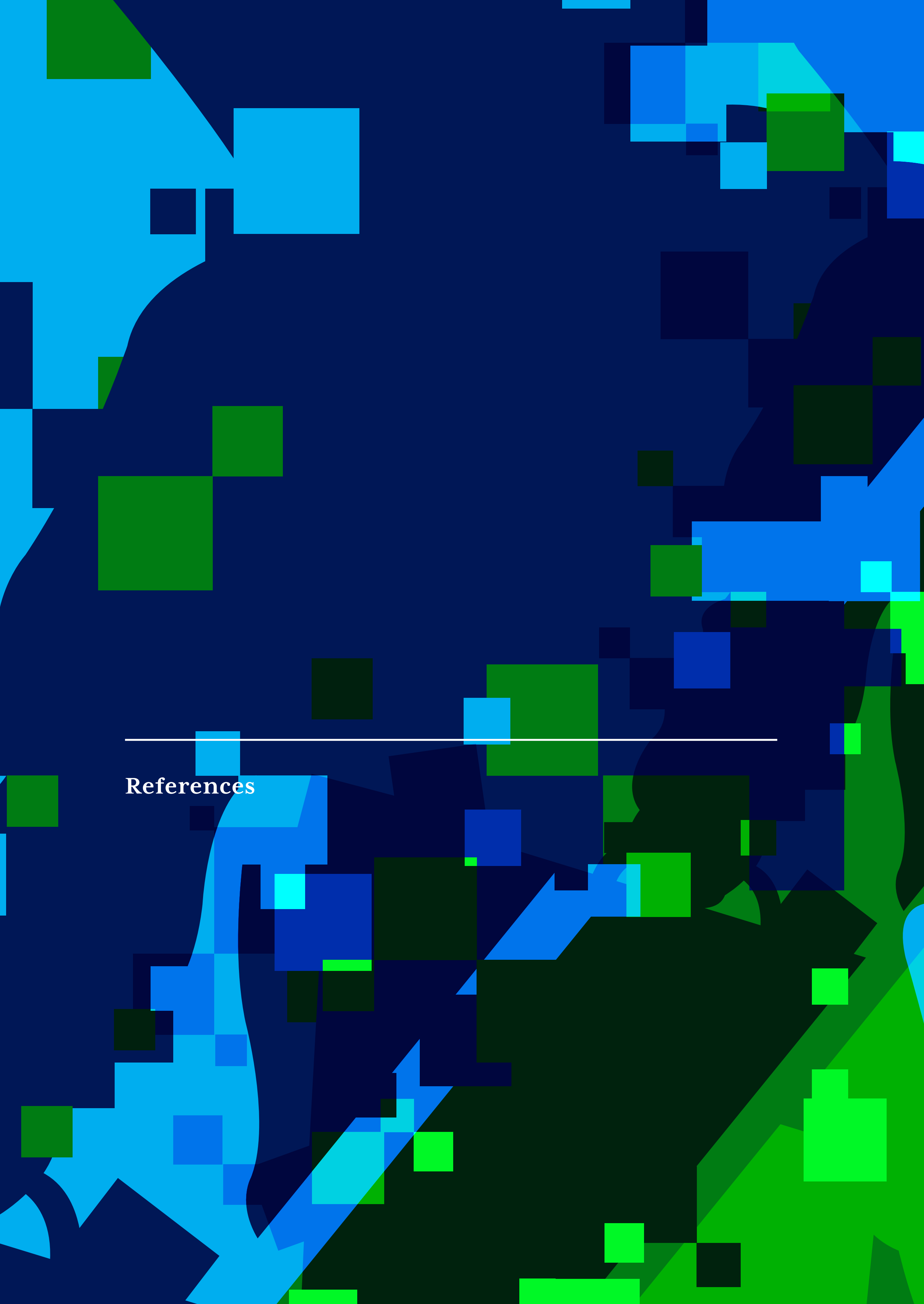
Subsequently, interventions that increase the perceived consequences for the offender and his or her victim may be helpful, as theories suggest that offending is more easy online, because there are no real consequences and victims are invisible (e.g., Jaishankar, 2009; Suler, 2004). Situational prevention could, for example, increase the offender's perception of the risk of being detected and prosecuted. An example of such a situational approach is the use of a warning banner that indicates the surveillance of all processes on an IT-system and the likely consequences of the illegal use of that IT-system by the offender (e.g., Howell, Cochran, Powers, Maimon, & Jones, 2017; Maimon et al., 2014; Wilson, Maimon, Sobesto, & Cukier, 2015). Interestingly, Jones (2014) shows that it may be helpful to use these warning banners to de-anonymise the possible victim of an attack, for example by signing such a warning banner with 'Over-worked admin'.

Another way of increasing the risk perception of offenders is by so-called 'cease and desist visits' (National Crime Agency, 2017b). These may be a useful tool in preventing further and more serious offending of known offenders. In these 'cease and desist visits' an offender whose behaviour is not serious enough for arrest, has a face-to-face visit with a police officer. This visit shows that the offender's criminal behaviour does not go undetected and the offender is advised to desist from committing crimes in the future, to prevent arrest and other negative consequences. However, as discussed above, it is very important that this type of intervention also provides guidance in how to move from illegal use of IT-skills to responsible use of IT-skills. In addition, it is important that continuing offending after such a visit will actually result in a punishment. Otherwise, these visits will lose their impact in the future.

For cybercrime, a promising way of helping offenders to move from the illegal use of IT to responsible use of IT is by assigning offenders to a mentor. In contrast to traditional crime, it seems less effective for cybercrime to reduce the influence of real-world same-aged deviant peers. This dissertation indicated that older role models seem to have the most impact on cyber-offending and this could therefore be used in an intervention. An offender could be assigned to a mentor, a legitimate white hat hacker, for example, who provides guidance in ways to enhance cybersecurity without misusing IT-systems and without causing any damage.

Such a mentor could, for example, explain the guidelines for 'Responsible Disclosure' (National Cyber Security Centre, 2016). 'Responsible Disclosure' is a *'practice of responsibly reporting any security leaks found. Responsible disclosure is based on agreements that usually mean that a reporter will not share his discovery with third parties until the leak has been repaired, and the affected party will not take legal action against the reporter'* (p. 89). By adhering to the rules of Responsible Disclosure, ex-offenders could still try to find vulnerabilities and thereby satisfy their curiosity and need for enhancing their IT-skills, without any negative consequences. In these types of intervention that focus on increasing legitimate use of IT and the perception of consequences of illegitimate use, it could be useful to know that this dissertation indicated that the offenders who commit the more technical types of crime, have a relatively higher self-control compared to the offenders who commit less technical types of crime. Therefore, their behaviour may be more rational than the behaviour of other offenders and they may be better able to assess the different ways in which they could act responsibly after they discover a vulnerability.

Lastly, in an attempt to reduce the prevalence of cybercrime in the future, young people should not only learn IT-skills, but also responsible ways of using those skills. Right now, general prevention programs against cybercrime generally focus on techniques to prevent victimisation and, for example, schools start including programming and other IT-skills in their educational program. These general prevention programs are important to increase resilience against cyberattacks in the future, but ethics and other aspects of responsible IT-use should be an important component of these programs as well. Otherwise, young people will learn IT-skills without learning how to use them responsibly. Educational institutes already adopted several ways of addressing their students' offline risk behaviour and they should now adopt their strategies to behaviour in the digital world as well. In that way educational programs may be able to reduce their students offending in the present, and maybe even provide them with the skills and ethics that could reduce the prevalence and impact of new types of cyber-dependent offending that will arise in the future.



References

Agnew, R. (1991). The Interactive Effects of Peer Variables on Delinquency. *Criminology, 29*(1), 47-72.

Akers, R. L. (1998). *Social Learning and Social Structure: A General Theory of Crime and Deviance*. Boston: Northeastern University Press.

Alleyne, B. (2011). *"We Are All Hackers Now": Critical Sociological Reflections on the Hacking Phenomenon*. Goldsmiths Research Online. Retrieved from http://www.arifyildirim.com/ilt510/brian.alleyne.pdf.

Averdijk, M., Van Gelder, J. L., Eisner, M., & Ribeaud, D. (2016). Violence Begets Violence... but How? A Decision-Making Perspective on the Victim-Offender Overlap. *Criminology, 54*(2), 282-306.

Bachmann, M. (2010). The Risk Propensity and Rationality of Computer Hackers. *International Journal of Cyber Criminology, 4*(1), 643-656.

Bachmann, M. (2011). Deciphering the Hacker Underground: First Quantitative Insights. In T. J. Holt & B. H. Schell (Eds.), *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications* (pp. 105-126). New York: Information Science Reference.

Bachmann, M., & Corzine, J. (2010). Insights into the Hacking Underground. In T. Finnie, T. Petee, & J. Jarvis (Eds.), *The Future Challenges of Cybercrime. Volume 5: Proceedings of the Futures Working Group 2010.* (pp. 31-41). Quantico, VA: FBI.

Baltagi, B. (2005). *Econometric Analysis of Panel Data* (3 ed.). West Sussex: John Wiley & Sons.

Berg, M. T., & Felson, R. B. (2016). Why Are Offenders Victimized So Often? In C. A. Cuevas & C. M. Rennison (Eds.), *The Wiley Handbook on the Psychology of Violence* (pp. 49-65). West Sussex, UK: John Wiley & Sons, Ltd.

Berg, M. T., Stewart, E. A., Schreck, C. J., & Simons, R. L. (2012). The Victim–Offender Overlap in Context: Examining the Role of Neighborhood Street Culture. *Criminology, 50*(2), 359-390.

Bernaards, F., Monsma, E., & Zinn, P. (2012). *High Tech Crime. Criminaliteitsbeeldanalyse 2012*. Retrieved from https://www.politie.nl/binaries/content/assets/politie/algemeen/nationaal-dreigingsbeeld-2012/cba-hightechcrime.pdf.

Bernasco, W. (2010a). A Sentimental Journey to Crime: Effects of Residential History on Crime Location Choice. *Criminology, 48*(2), 389-416.

Bernasco, W. (2010b). *Offenders on Offending: Learning About Crime from Criminals*. New York: Taylor & Francis US.

Bernasco, W., Ruiter, S., Bruinsma, G. J. N., Pauwels, L. J. R., & Weerman, F. M. (2013). Situational Causes of Offending: A Fixed-Effects Analysis of Space–Time Budget Data. *Criminology, 51*(4), 895-926.

Blackburn, J., Kourtellis, N., Skvoretz, J., Ripeanu, M., & Iamnitchi, A. (2014). Cheating in Online Games: A Social Network Perspective. *Acm Transactions on Internet Technology, 13*(3), 1-25.

Blokland, A. A. J. (2014). School, Intensive Work, Excessive Alcohol Use and Delinquency During Emerging Adulthood. In F. M. Weerman & C. Bijleveld (Eds.), *Criminal Behaviour from School to the Workplace: Untangling the Complex Relations between Employment, Education and Crime* (pp. 87-107). New York: Routledge.

Blokland, A. A. J., & Nieuwbeerta, P. (2005). The Effects of Life Circumstances on Longitudinal Trajectories of Offending. *Criminology, 43*(4), 1203-1240.

Boman, J. H. (2016). Do Birds of a Feather Really Flock Together? Friendships, Self-Control Similarity and Deviant Behaviour. *British Journal of Criminology, 57*(5), 1208–1229.

Boman, J. H., Rebellon, C. J., & Meldrum, R. C. (2016). Can Item-Level Error Correlations Correct for Projection Bias in Perceived Peer Deviance Measures? A Research Note. *Journal of Quantitative Criminology, 32*(1), 89-102.

Bossler, A. M., & Burruss, G. W. (2011). The General Theory of Crime and Computer Hacking: Low Self-Control Hackers? In T. J. Holt & B. H. Schell (Eds.), *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications* (pp. 38-67). New York: Information Science Reference.

Bossler, A. M., & Holt, T. J. (2009). On-Line Activities, Guardianship, and Malware Infection: An Examination of Routine Activities Theory. *International Journal of Cyber Criminology, 3*(1), 400-420.

Bossler, A. M., & Holt, T. J. (2010). The Effect of Self-Control on Victimization in the Cyberworld. *Journal of Criminal Justice, 38*(3), 227-236.

Brady, P. Q., Randa, R., & Reyns, B. W. (2016). From WWII to the World Wide Web. *Journal of Contemporary Criminal Justice, 32*(2), 129-147.

Brechwald, W. A., & Prinstein, M. J. (2011). Beyond Homophily: A Decade of Advances in Understanding Peer Influence Processes. *Journal of Research on Adolescence, 21*(1), 166-179.

Brenner, S. W. (2006). Cybercrime Jurisdiction. *Crime Law and Social Change, 46*(4-5), 189-206.

Brüderl, J., & Ludwig, V. (2014). Fixed-Effects Panel Regression. In H. Best & C. Wolf (Eds.), *The Sage Handbook of Regression Analysis and Causal Inference* (pp. 327-358). London: Sage.

Campbell, Q., & Kennedy, D. M. (2012). The Psychology of Computer Criminals. In S. Bosworth, M. E. Kabay, & E. Whyne (Eds.), *Computer Security Handbook* (pp. 12.11-12.33). Hoboken, New Jersey: John Wiley & Sons, Inc.

Cappellari, L., & Jenkins, S. P. (2003). Multivariate Probit Regression Using Simulated Maximum Likelihood. *Stata journal, 3*(3), 278-294.

Chan, D., & Wang, D. (2015). Profiling Cybercrime Perpetrators in China and Its Policy Countermeasures. In R. G. Smith, R. C.-C. Cheung, & L. Y.-C. Lau (Eds.), *Cybercrime Risks and Responses: Eastern and Western Perspectives* (pp. 206-221). London: Palgrave Macmillan UK.

Chiesa, R., Ducci, S., & Ciappi, S. (2008a). Appendix C: The Nine Hacker Categories. In R. Chiesa, S. Ducci, & S. Ciappi (Eds.), *Profiling Hackers: The Science of Criminal Profiling as Applied to the World of Hacking* (pp. 239-241). Boca Raton: CRC Press.

Chiesa, R., Ducci, S., & Ciappi, S. (2008b). *Profiling Hackers: The Science of Criminal Profiling as Applied to the World of Hacking*. Boca Raton: CRC Press.

Chiesa, R., Ducci, S., & Ciappi, S. (2008c). Who Are Hackers? Part 2. In R. Chiesa, S. Ducci, & S. Ciappi (Eds.), *Profiling Hackers: The Science of Criminal Profiling as Applied to the World of Hacking* (pp. 121-188). Boca Raton: CRC Press.

Chiesa, R., Ducci, S., & Ciappi, S. (2008d). To Be, Think, and Live as a Hacker. In R. Chiesa, S. Ducci, & S. Ciappi (Eds.), *Profiling Hackers: The Science of Criminal Profiling as Applied to the World of Hacking* (pp. 33-56). Boca Raton: CRC Press.

Choi, K.-S. (2008). Computer Crime Victimization and Integrated Theory: An Empirical Assessment. *International Journal of Cyber Criminology, 2*(1), 308-333.

Chua, Y.-T., & Holt, T. J. (2016). A Cross-National Examination of the Techniques of Neutralization to Account for Hacking Behaviors. *Victims & Offenders, 11*(4), 534-555.

Cohen, L. E., & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review, 44*(4), 588-608.

Dalal, A. S., & Sharma, R. (2007). Peeping into a Hacker's Mind: Can Criminological Theories Explain Hacking? *ICFAI Journal of Cyber Law, 6*(4), 34-47.

De Vries, R. E., & Born, M. P. (2013). The Simplified Hexaco Personality Questionnaire and an Additional Intertitial Proactivity Facet [De Vereenvoudigde Hexaco Persoonlijkheidsvragenlijst En Een Additioneel Interstitieel Proactiviteitsfacet]. *Gedrag & Organisatie, 26*(2), 223-245.

Denning, D. E. (2011). Cyber Conflict as an Emergent Social Phenomenon. In T. J. Holt & B. H. Schell (Eds.), *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications* (pp. 170-186). New York: Information Science Reference.

Dirkzwager, A. J. E., & Nieuwbeerta, P. (2015). *Prison Project: Codebook and Documentation-D1 Interview.* Leiden University/NSCR. Leiden/Amsterdam, The Netherlands.

Domenie, M. M. L., Leukfeldt, E. R., Van Wilsem, J. A., Jansen, J., & Stol, W. P. (2013). *Victimization in a Digital Society [Slachtofferschap in Een Gedigitaliseerde Samenleving]*. Den Haag: Boom Lemma.

Donner, C. M., Marcum, C. D., Jennings, W. G., Higgins, G. E., & Banfield, J. (2014). Low Self-Control and Cybercrime: Exploring the Utility of the General Theory of Crime Beyond Digital Piracy. *Computers in Human Behavior, 34*, 165-172.

European Cybercrime Center. (2014). *The Internet Organized Crime Threat Assessment (Iocta)*. Retrieved from https://www.europol.europa.eu/sites/default/files/publications/europol_iocta_web.pdf.

Flashman, J., & Gambetta, D. (2014). Thick as Thieves: Homophily and Trust among Deviants. *Rationality and Society, 26*(1), 3-45.

Ford, J. A., & Schroeder, R. D. (2010). Higher Education and Criminal Offending over the Life Course. *Sociological Spectrum, 31*(1), 32-58.

Fotinger, C., & Ziegler, W. (2004). *Understanding a Hacker's Mind: A Psychological Insight into the Hijacking of Identities*. Retrieved from http://www.donau-uni.ac.at/de/department/gpa/informatik/DanubeUniversityHackersStudy.pdf.

Furnell, S. M. (2002). Categorising Cybercrime and Cybercriminals: The Problem and Potential Approaches. *Journal of Information Warfare, 1*(5), 35-44.

Goldsmith, A., & Brewer, R. (2015). Digital Drift and the Criminal Interaction Order. *Theoretical Criminology, 19*(1), 112-130.

Gordon, S., & Ford, R. (2006). On the Definition and Classification of Cybercrime. *Journal in Computer Virology, 2*(1), 13-20.

Gordon, S., & Ma, Q. (2003). *Convergence of Virus Writers and Hackers: Fact or Fantasy?* Retrieved from http://download.adamas.ai/dlbase/ebooks/VX_related/Convergence%20of%20Virus%20Writers%20and%20Hackers%20Fact%20or%20Fantasy.pdf.

Gottfredson, M. R., & Hirschi, T. (1990). *A General Theory of Crime*. Palo Alto, CA: Stanford University Press.

Grabosky, P. N. (2000). *Computer Crime: A Criminological Overview.* Paper presented at the Workshop on Crimes Related to the Computer Network, Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, Vienna.

Grabosky, P. N. (2001). Virtual Criminality: Old Wine in New Bottles? *Social & Legal Studies, 10*(2), 243-249.

Grabosky, P. N. (2017). The Evolution of Cybercrime, 2006-2016. In T. J. Holt (Ed.), *Cybercrime through an Interdisciplinary Lens* (pp. 15-36). New York: Routledge.

Grabosky, P. N., & Walkley, S. (2007). Computer Crime and White-Collar Crime. In H. N. Pontell & G. L. Geis (Eds.), *International Handbook of White-Collar and Corporate Crime* (pp. 358-375). New Yorl: Springer US.

Grasmick, H. G., Tittle, C. R., Bursik, R. J., & Arneklev, B. J. (1993). Testing the Core Empirical Implications of Gottfredson and Hirschi's General Theory of Crime. *Journal of Research in Crime and Delinquency, 30*(1), 5-29.

Hay, C., & Evans, M. M. (2006). Violent Victimization and Involvement in Delinquency: Examining Predictions from General Strain Theory. *Journal of Criminal Justice, 34*(3), 261-274.

Haynie, D. L., & Kreager, D. A. (2013). Peer Networks and Crime. In F. T. Cullen & P. Wilcox (Eds.), *The Oxford Handbook of Criminological Theory* (pp. 257-273). Oxford: Oxford University Press.

Hirschi, T. (1969). *Causes of Delinquency*. Berkeley, CA: University of California press.

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

Holt, T. J. (2007). Subcultural Evolution? Examining the Influence of on- and Off-Line Experiences on Deviant Subcultures. *Deviant Behavior, 28*(2), 171-198.

Holt, T. J. (2009a). Lone Hacks or Group Cracks: Examining the Social Organization of Computer Hackers. In F. Schmalleger & M. Pittaro (Eds.), *Crimes of the Internet* (pp. 336-355). New Jersey: Pearson Education.

Holt, T. J. (2009b). *The Attack Dynamics of Political and Religiously Motivated Hackers.* Paper presented at the Cyber Infrastructure Protection Conference, New York.

Holt, T. J., & Bossler, A. M. (2008). Examining the Applicability of Lifestyle-Routine Activities Theory for Cybercrime Victimization. *Deviant Behavior, 30*(1), 1-25.

Holt, T. J., & Bossler, A. M. (2014). An Assessment of the Current State of Cybercrime Scholarship. *Deviant Behavior, 35*(1), 20-40.

Holt, T. J., Bossler, A. M., & May, D. C. (2012). Low Self-Control, Deviant Peer Associations, and Juvenile Cyberdeviance. *American Journal of Criminal Justice, 37*(3), 378-395.

Holt, T. J., Burruss, G. W., & Bossler, A. M. (2010). Social Learning and Cyber-Deviance: Examining the Importance of a Full Social Learning Model in the Virtual World. *Journal of Crime and Justice, 33*(2), 31-61.

Holt, T. J., & Kilger, M. (2008). *Techcrafters and Makecrafters: A Comparison of Two Populations of Hackers.* Paper presented at the WOMBAT Workshop on Information Security Threats Data Collection and Sharing, 2008. WISTDCS'08, Amsterdam.

Holt, T. J., & Kilger, M. (2012). Know Your Enemy: The Social Dynamics of Hacking. *The Honeynet Project.* Retrieved from https://honeynet.org/papers/socialdynamics.

Holt, T. J., Smirnova, O., & Chua, Y.-T. (2016). *Data Thieves in Action: Examining the International Market for Stolen Personal Information*. New York: Palgrave Macmillan US.

Holt, T. J., Strumsky, D., Smirnova, O., & Kilger, M. (2012). Examining the Social Networks of Malware Writers and Hackers. *International Journal of Cyber Criminology, 6*(1), 891-903.

Holtfreter, K., Reisig, M. D., & Pratt, T. C. (2008). Low Self-Control, Routine Activities, and Fraud Victimization. *Criminology, 46*(1), 189-220.

Howell, C. J., Cochran, J. K., Powers, R. A., Maimon, D., & Jones, H. M. (2017). System Trespasser Behavior after Exposure to Warning Messages at a Chinese Computer Network: An Examination. *International Journal of Cyber Criminology, 11*(1), 63-77.

Hu, Q., Xu, Z., & Yayla, A. A. (2013). *Why College Students Commit Computer Hacks: Insights from a Cross Culture Analysis.* Paper presented at the Pacific Asia Conference on Information Systems (PACIS), Jeju Island, Korea.

Hutchings, A. (2014). Crime from the Keyboard: Organised Cybercrime, Co-Offending, Initiation and Knowledge Transmission. *Crime Law and Social Change, 62*(1), 1-20.

Hutchings, A., & Clayton, R. (2016). Exploring the Provision of Online Booter Services. *Deviant Behavior, 37*(10), 1163-1178.

Ibrahim, S. (2016). Social and Contextual Taxonomy of Cybercrime: Socioeconomic Theory of Nigerian Cybercriminals. *International Journal of Law, Crime and Justice, 47*(2016), 44-57.

Internet Live Stats. (2017). Internet Users. Retrieved from http://www.internetlivestats.com/internet-users/.

Jaishankar, K. (2009). Space Transition Theory of Cyber Crimes. In F. Schmalleger & M. Pittaro (Eds.), *Crimes of the Internet* (pp. 283-301). New Jersey: Pearson Education.

Jennings, W. G., Higgins, G. E., Tewksbury, R., Gover, A. R., & Piquero, A. R. (2010). A Longitudinal Assessment of the Victim-Offender Overlap. *Journal of Interpersonal Violence, 25*(12), 2147-2174.

Jennings, W. G., Piquero, A. R., & Reingle, J. M. (2012). On the Overlap between Victimization and Offending: A Review of the Literature. *Aggression and Violent Behavior, 17*(1), 16-26.

Jensen, G. F., & Brownfield, D. (1986). Gender, Lifestyles, and Victimization: Beyond Routine Activity. *Violence and victims, 1*(2), 85-99.

Jones, H. M. (2014). *The Restrictive Deterrent Effect of Warning Messages on the Behavior of Computer System Trespassers.* University of Maryland, ProQuest LLC. Ann Arbor. Retrieved from http://drum.lib.umd.edu/bitstream/handle/1903/15544/Jones_umd_0117N_15230.pdf?sequence=1&isAllowed=y.

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

Kalmijn, M. (1998). Intermarriage and Homogamy: Causes, Patterns, Trends. *Annual Review of Sociology, 24*(1), 395-421.

Kandel, D. B. (1978). Homophily, Selection, and Socialization in Adolescent Friendships. *American Journal of Sociology, 84*(2), 427-436.

Kazemian, L. (2015). Desistance from Crime and Antisocial Behavior. In J. Morizot & L. Kazemian (Eds.), *The Development of Criminal and Antisocial Behavior* (pp. 295-312). New York: Springer.

Kerstens, J., & Jansen, J. (2016). The Victim–Perpetrator Overlap in Financial Cybercrime: Evidence and Reflection on the Overlap of Youth's on-Line Victimization and Perpetration. *Deviant Behavior, 37*(5), 585-600.

Kilger, M. (2011). Social Dynamics and the Future of Technolgy-Driven Crime. In T. J. Holt & B. H. Schell (Eds.), *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications* (pp. 205-227). New York: Information Science Reference.

Kilger, M., Arkin, O., & Stutzman, J. (2004). Profiling. In The Honeynet Project (Ed.), *Know Your Enemy: Learning About Security Threats* (2 ed.). Boston: Addison-Wesley Professional.

Kirwan, G., & Power, A. (2013). *Cybercrime: The Psychology of Online Offenders*. Cambridge: Cambridge University Press.

Kshetri, N. (2009). Positive Externality, Increasing Returns, and the Rise in Cybercrimes. *Communications of the ACM, 52*(12), 141-144.

Kshetri, N. (2013). Cybercrimes in the Former Soviet Union and Central and Eastern Europe: Current Status and Key Drivers. *Crime Law and Social Change, 60*(1), 39-65.

Lageson, S., & Uggen, C. (2013). How Work Affects Crime - and Crime Affects Work - over the Life Course. In C. L. Gibson & M. D. Krohn (Eds.), *Handbook of Life-Course Criminology* (pp. 201-212). New York: Springer.

Lauritsen, J. L., & Laub, J. H. (2007). Understanding the Link between Victimization and Offending: New Reflections on an Old Idea. In M. Hough & M. Maxfield (Eds.), *Surveying Crime in the 21st Century* (Vol. 22, pp. 55-75). Monsey, NY, USA: Criminal Justice Press.

Lauritsen, J. L., Sampson, R. J., & Laub, J. H. (1991). The Link between Offending and Victimization among Adolescents. *Criminology, 29*(2), 265-292.

Leukfeldt, E. R. (2014). Phishing for Suitable Targets in the Netherlands: Routine Activity Theory and Phishing Victimization. *Cyberpsychology Behavior and Social Networking, 17*(8), 551-555.

Leukfeldt, E. R., Lavorgna, A., & Kleemans, E. R. (2016). Organised Cybercrime or Cybercrime That Is Organised? An Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime. *European Journal on Criminal Policy and Research, 23*(3), 287–300.

Leukfeldt, E. R., Veenstra, S., & Stol, W. P. (2013). High Volume Cyber Crime and the Organization of the Police: The Results of Two Empirical Studies in the Netherlands. *International Journal of Cyber Criminology, 7*(1), 1-17.

Leukfeldt, E. R., & Yar, M. (2016). Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis. *Deviant Behavior, 37*(3), 263-280.

Longshore, D., Chang, E., Hsieh, S.-c., & Messina, N. (2004). Self-Control and Social Bonds: A Combined Control Perspective on Deviance. *Crime & Delinquency, 50*(4), 542-564.

Lu, C., Jen, W., Chang, W., & Chou, S. (2006). Cybercrime & Cybercriminals: An Overview of the Taiwan Experience. *Journal of Computers, 1*(6), 11-18.

Maimon, D., Alper, M., Sobesto, B., & Cukier, M. (2014). Restrictive Deterrent Effects of a Warning Banner in an Attacked Computer System. *Criminology, 52*(1), 33-59.

Maimon, D., Kamerdze, A., Cukier, M., & Sobesto, B. (2013). Daily Trends and Origin of Computer-Focused Crimes against a Large University Computer Network: An Application of the Routine-Activities and Lifestyle Perspective. *British Journal of Criminology, 53*(2), 319-343.

Marcum, C. D., Higgins, G. E., Ricketts, M. L., & Wolfe, S. E. (2014). Hacking in High School: Cybercrime Perpetration by Juveniles. *Deviant Behavior, 35*(7), 581-591.

McCallister, L., & Fischer, C. S. (1978). A Procedure for Surveying Personal Networks. *Sociological Methods & Research, 7*(2), 131-148.

McGloin, J. M., & Shermer, L. O. N. (2009). Self-Control and Deviant Peer Network Structure. *Journal of Research in Crime and Delinquency, 46*(1), 35-72.

McGuire, M., & Dowling, S. (2013). *Chapter 1: Cyber-Dependent Crimes.* Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/246751/horr75-chap1.pdf.

McPherson, M., Smith-Lovin, L., & Cook, J. M. (2001). Birds of a Feather: Homophily in Social Networks. *Annual Review of Sociology, 27*(1), 415-444.

Morris, R. G. (2011). Computer Hacking and the Techniques of Neutralization: An Empirical Assessment. In T. J. Holt & B. H. Schell (Eds.), *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications* (pp. 1-17). New York: Information Science Reference.

Morris, R. G., & Blackburn, A. G. (2009). Cracking the Code: An Emperical Exploration of Social Learning Theory and Computer Crime. *Journal of Crime and Justice, 32*(1), 1-34.

National Crime Agency. (2017a). *Identify, Intervene, Inspire: Helping Young People to Pursue Careers in Cyber Security, Not Cyber Crime*. Retrieved from https://www.crest-approved.org/wp-content/uploads/CREST_NCA_CyberCrimeReport.pdf.

National Crime Agency. (2017b). *Pathways into Cyber Crime*. Retrieved from http://www.nationalcrimeagency.gov.uk/publications/791-pathways-into-cyber-crime/file.

National Cyber Security Centre. (2012). *Cybercrime: From Recognition to Report [Cybercrime. Van Herkenning Tot Aangifte]*. Retrieved from https://www.ncsc.nl/binaries/content/documents/ncsc-nl/actueel/nieuwsberichten/publicatie-cybercrime/1/Handreiking%2BCybercrime.pdf.

National Cyber Security Centre. (2016). *Cyber Security Assessment Netherlands*. Retrieved from https://www.ncsc.nl/binaries/content/documents/ncsc-en/current-topics/cyber-security-assessment-netherlands/cyber-security-assessment-netherlands-2016/1/CSAN2016.pdf.

Ngo, F. T., & Paternoster, R. (2011). Cybercrime Victimization: An Examination of Individual and Situational Level Factors. *International Journal of Cyber Criminology, 5*(1), 773-793.

Nycyk, M. (2010). *Computer Hackers in Virtual Community Forums: Identity Shaping and Dominating Other Hackers*. Paper presented at the Online Conference on Networks and Communities: Debating Communities and Networks.

Nykodym, N., Taylor, R., & Vilela, J. (2005). Criminal Profiling and Insider Cyber Crime. *Computer Law & Security Review, 21*(5), 408-414.

Office for National Statistics. (2015). Improving Crime Statistics in England and Wales. *Crime Statistics, Year Ending June 2015 Release*. Retrieved from 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, G. C., Wilcox, P., & Fisher, B. S. (2011). Something Old, Something New: Revisiting Competing Hypotheses of the Victimization-Offending Relationship among Adolescents. *Journal of Quantitative Criminology, 27*(1), 53-84.

Parker, D. B. (1983). *Fighting Computer Crime*. New York, NY: Scribner.

Payne, A. A., & Welch, K. (2015). How School and Education Impact the Development of Criminal and Antisocial Behavior. In J. Morizot & L. Kazemian (Eds.), *The Development of Criminal and Antisocial Behavior* (pp. 237-251). New York: Springer.

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

Pontell, H., & Rosoff, S. (2009). White-Collar Delinquency. *Crime Law and Social Change, 51*(1), 147-162.

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

Pratt, T. C., Cullen, F. T., Sellers, C. S., Winfree, L. T., Madensen, T. D., Daigle, L. E., Fearn, N. E., & Gau, J. M. (2009). The Empirical Status of Social Learning Theory: A Meta-Analysis. *Justice Quarterly, 27*(6), 765-802.

Pratt, T. C., Turanovic, J. J., Fox, K. A., & Wright, K. A. (2014). Self-Control and Victimization: A Meta-Analysis. *Criminology, 52*(1), 87-116.

Provos, N., Rajab, M. A., & Mavrommatis, P. (2009). Cybercrime 2.0: When the Cloud Turns Dark. *Communications of the ACM, 52*(4), 42-47.

Randazzo, M. R., Keeney, M., Kowalski, E., Cappelli, D., & Moore, A. (2005). *Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector*. Retrieved from http://www.dtic.mil/dtic/tr/fulltext/u2/a441249.pdf.

Rogers, M. K. (2000). A New Hacker Taxonomy. *Telematic Journal of Clinical Criminology*.

Rogers, M. K. (2001). A Social Learning Theory and Moral Disengagement Analysis of Criminal Computer Behavior: An Exploratory Study. Retrieved from https://www.cerias.purdue.edu/assets/pdf/bibtex_archive/rogers_01.pdf.

Rogers, M. K. (2006). A Two-Dimensional Circumplex Approach to the Development of a Hacker Taxonomy. *Digital Investigation, 3*(2), 97-102.

Rogers, M. K. (2011). The Psyche of Cybercriminals: A Psycho-Social Perspective. In S. Ghosh & E. Turrini (Eds.), *Cybercrimes: A Multidisciplinary Analysis* (pp. 217-235). Berlin, Heidelberg: Springer Berlin Heidelberg.

Rokven, J. J., De Boer, G., Tolsma, J., & Ruiter, S. (2017). How Friends' Involvement in Crime Affects the Risk of Offending and Victimization. *European Journal of Criminology,* (First published online December 28, 2016), 1-23.

Rokven, J. J., Tolsma, J., Ruiter, S., & Kraaykamp, G. (2016). Like Two Peas in a Pod? Explaining Friendship Selection Processes Related to Victimization and Offending. *European Journal of Criminology, 13*(2), 231-256.

Royston, P. (2004). Multiple Imputation of Missing Values. *Stata journal, 4*(3), 227-241.

Rubin, D. B. (1987). *Multiple Imputation for Nonresponse in Surveys*. New York: Wiley & Sons.

Ruiter, S., & Bernaards, F. (2013). Are Crackers Different from Other Criminals? A Comparison Based on Dutch Suspect Registrations [Verschillen Crackers Van Andere Criminelen? Een Vergelijking Op Basis Van Nederlandse Verdachtenregistraties]. *Tijdschrift voor Criminologie, 55*(4), 342-359.

Sampson, R. J., & Laub, J. H. (1993). *Crime in the Making: Pathways and Turning Points through Life*. Cambridge: Harvard University Press.

Sampson, R. J., & Lauritsen, J. L. (1990). Deviant Lifestyles, Proximity to Crime, and the Offender-Victim Link in Personal Violence. *Journal of Research in Crime and Delinquency, 27*(2), 110-139.

Schreck, C. J. (1999). Criminal Victimization and Low Self-Control: An Extension and Test of a General Theory of Crime. *Justice Quarterly, 16*(3), 633-654.

Schreck, C. J., Stewart, E. A., & Fisher, B. S. (2006). Self-Control, Victimization, and Their Influence on Risky Lifestyles: A Longitudinal Analysis Using Panel Data. *Journal of Quantitative Criminology, 22*(4), 319-340.

Schreck, C. J., Stewart, E. A., & Osgood, D. W. (2008). A Reappraisal of the Overlap of Violent Offenders and Victims. *Criminology, 46*(4), 871-906.

Schreck, C. J., Wright, R. A., & Miller, J. M. (2002). A Study of Individual and Situational Antecedents of Violent Victimization. *Justice Quarterly, 19*(1), 159-180.

Seebruck, R. (2015). A Typology of Hackers: Classifying Cyber Malfeasance Using a Weighted Arc Circumplex Model. *Digital Investigation, 14*(2015), 36-45.

Skardhamar, T., Savolainen, J., Aase, K. N., & Lyngstad, T. H. (2015). Does Marriage Reduce Crime? *Crime & Justice, 44*(1), 385-557.

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

Smith, R. G. (2015). Trajectories of Cybercrime. In R. G. Smith, R. C.-C. Cheung, & L. Y.-C. Lau (Eds.), *Cybercrime Risks and Responses: Eastern and Western Perspectives* (pp. 13-34). London: Palgrave Macmillan UK.

Statistics Netherlands. (2014a). Dutch Labour Force Survey (Lfs). Retrieved from http://www.cbs.nl/en-GB/menu/methoden/dataverzameling/dutch-labour-force-survey-characteristics.htm.

Statistics Netherlands. (2014b). Standard Industrial Classifications (Dutch Sbi 2008, Nace and Isic). Retrieved from http://www.cbs.nl/en-GB/menu/methoden/classificaties/overzicht/sbi/default.htm?Languageswitch=on.

Statistics Netherlands. (2014c). *Safetymonitor 2014 [Veiligheidsmonitor 2014]*. Retrieved from http://download.cbs.nl/pdf/veiligheidsmonitor-2014.pdf.

Statistics Netherlands. (2015a). Registered Crime; Type of Crime, Region (Format 2015) [Geregistreerde Criminaliteit; Soort Misdrijf, Regio (Indeling 2015)]. Retrieved 16 January 2017, from Statistics Netherlands [Centraal Bureau voor de Statistiek (CBS)], http://statline.cbs.nl/Statweb/publication/?VW=T&DM=SLNL&PA=83032NED&D1=0-5&D2=0,31&D3=0&D4=a&HD=150715-1325&HDR=T&STB=G2,G1,G3.

Statistics Netherlands. (2015b). Ict Usage by Individuals and Individual Characteristics [Ict Gebruik Van Personen Naar Persoonskenmerken]. Retrieved 16 January 2017, from Statistics Netherlands [Centraal Bureau voor de Statistiek (CBS)], http://statline.cbs.nl/Statweb/publication/?VW=T&DM=SLNL&PA=71098ned&D1=7-14,21-26,69-84&D2=8-16,25-28&D3=l&HD=150807-1532&HDR=G1,G2&STB=T&CHARTTYPE=1.

Statistics Netherlands. (2017). *Safetymonitor 2016 [Veiligheidsmonitor 2016]*. Retrieved from http://www.veiligheidsmonitor.nl/dsresource?objectid=885.

Steinberg, L., & Monahan, K. C. (2007). Age Differences in Resistance to Peer Influence. *Developmental Psychology, 43*(6), 1531-1543.

Stephenson, P., & Walter, R. (2012). *Cyber Crime Assessment.* Paper presented at the 45th Hawaii International Conference on System Science (HICSS), Grand Wailea, Maui, Hawaii.

Stol, W. P., Leukfeldt, E. R., & Domenie, M. M. L. (2010). *Cybercrime in the Netherlands 2009. A Picture on the Basis of Police Files.* Paper presented at the third Giganet workshop, Montreal, Canada.

Stouthamer–Loeber, M., Wei, E., Loeber, R., & Masten, A. S. (2004). Desistance from Persistent Serious Delinquency in the Transition to Adulthood. *Development and Psychopathology, 16*(4), 897-918.

Suler, J. (2004). The Online Disinhibition Effect. *CyberPsychology & behavior, 7*(3), 321-326.

Svensson, R., Weerman, F. M., Pauwels, L. J. R., Bruinsma, G. J. N., & Bernasco, W. (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.

Sykes, G. M., & Matza, D. (1957). Techniques of Neutralization: A Theory of Delinquency. *American Sociological Review, 22*(6), 664-670.

Taylor, P. A. (1999). *Hackers: Crime in the Digital Sublime*. London: Routledge.

Tcherni, M., Davies, A., Lopes, G., & Lizotte, A. (2016). The Dark Figure of Online Property Crime: Is Cyberspace Hiding a Crime Wave? *Justice Quarterly, 33*(5), 890-911.

Tonry, M. (2014). Why Crime Rates Are Falling Throughout the Western World. In M. Tonry (Ed.), *Crime and Justice, Vol 43: Why Crime Rates Fall, and Why They Don't* (Vol. 43, pp. 1-63). Chicago: Univ Chicago Press.

Turanovic, J. J., & Pratt, T. C. (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), 321-345.

Turgeman-Goldschmidt, O. (2008). Meanings That Hackers Assign to Their Being a Hacker. *International Journal of Cyber Criminology, 2*(2), 382-396.

Turgeman-Goldschmidt, O. (2009). The Rhetoric of Hackers' Neutralizations. In F. Schmalleger & M. Pittaro (Eds.), *Crimes of the Internet* (pp. 317-335). New Jersey: Pearson Education.

Turgeman-Goldschmidt, O. (2011). Between Hackers and White-Collar Offenders. In T. J. Holt & B. H. Schell (Eds.), *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications* (pp. 18-37). New York: Information Science Reference.

UNESCO. (1997). *International Standard Classification of Education Isced 1997*. Paris: United Nations Educational, Scientific and Cultural Organization.

Van Gelder, J. L., Averdijk, M., Eisner, M., & Ribeaud, D. (2015). Unpacking the Victim-Offender Overlap: On Role Differentiation and Socio-Psychological Characteristics. *Journal of Quantitative Criminology, 31*(4), 653-675.

Van Gelder, J. L., & De Vries, R. E. (2012). Traits and States: Integrating Personality and Affect into a Model of Criminal Decision Making. *Criminology, 50*(3), 637-671.

Van Wilsem, J. A. (2013). Hacking and Harassment—Do They Have Something in Common? Comparing Risk Factors for Online Victimization. *Journal of Contemporary Criminal Justice, 29*(4), 437-453.

Voiskounsky, A. E., & Smyslova, O. V. (2003). Flow-Based Model of Computer Hackers' Motivation. *CyberPsychology & behavior, 6*(2), 171-180.

Von Hippel, P. T. (2007). Regression with Missing Ys: An Improved Strategy for Analyzing Multiply Imputed Data. *Sociological Methodology, 37*(1), 83-117.

Wall, D. S. (2001). Cybercrimes and the Internet. *Crime and the Internet* (pp. 1-17). London: Routledge.

Warr, M. (1998). Life-Course Transitions and Desistance from Crime. *Criminology, 36*(2), 183-216.

Warr, M. (2002). *Companions in Crime: The Social Aspects of Criminal Conduct*. Cambridge: Cambridge University Press.

Weerman, F. M., & Smeenk, W. H. (2005). Peer Similarity in Delinquency for Different Types of Friends: A Comparison Using Two Measurement Methods. *Criminology, 43*(2), 499-524.

Weesie, J. (1999). Sg21: Seemingly Unrelated Estimation and the Cluster-Adjusted Sandwich Estimator. *Stata Technical Bulletin, 52*, 34-47.

Weulen Kranenbarg, M., Van Der Laan, A., De Poot, C., Verhoeven, M., Van Der Wagen, W., & Weijters, G. (2017). Individual Cybercrime Offenders. In E. R. Leukfeldt (Ed.), *Research Agenda: The Human Factor in Cybercrime and Cybersecurity*. Den Haag: Eleven International Publishing.

White, K. (2013). The Rise of Cybercrime 1970 Trough 2010. A Tour of the Conditions That Gave Rise to Cybercrime and the Crimes Themselves. Retrieved from http://www.slideshare.net/bluesme/the-rise-of-cybercrime-1970s-2010-29879338.

Wilcox, P., Land, K. C., & Hunt, S. A. (2003). *Criminal Circumstance: A Dynamic Multi-Contextual Criminal Opportunity Theory*. New York: Aldine de Gruyter.

Wilson, T., Maimon, D., Sobesto, B., & Cukier, M. (2015). The Effect of a Surveillance Banner in an Attacked Computer System. *Journal of Research in Crime and Delinquency, 52*(6), 829-855.

Wolfe, S. E., Higgins, G. E., & Marcum, C. D. (2008). Deterrence and Digital Piracy: A Preliminary Examination of the Role of Viruses. *Social Science Computer Review, 26*(3), 317-333.

Woo, H.-J. (2003). *The Hacker Mentality: Exploring the Relationship between Psychological Variables and Hacking Activities.* The University of Georgia, Athens, Georgia. Retrieved from https://getd.libs.uga.edu/pdfs/woo_hyung-jin_200305_phd.pdf.

Woo, H.-J., Kim, Y., & Dominick, J. (2004). Hackers: Militants or Merry Pranksters? A Content Analysis of Defaced Web Pages. *Media Psychology, 6*(1), 63-82.

Xu, Z., Hu, Q., & Zhang, C. (2013). Why Computer Talents Become Computer Hackers. *Communications of the ACM, 56*(4), 64-74.

Yar, M. (2005a). The Novelty of 'Cybercrime'. An Assessment in Light of Routine Activity Theory. *European Journal of Criminology, 2*(4), 407-427.

Yar, M. (2005b). Computer Hacking: Just Another Case of Juvenile Delinquency? *The Howard Journal of Criminal Justice, 44*(4), 387-399.

Yar, M. (2013a). Cybercrime and the Internet, an Introduction. In M. Yar (Ed.), *Cybercrime and Society* (2 ed., pp. 1-20). London: Sage.

Yar, M. (2013b). Hackers, Crackers and Viral Coders. . In M. Yar (Ed.), *Cybercrime and Society* (2 ed., pp. 21-43). London: Sage.

Young, J. T. N. (2011). How Do They 'End up Together'? A Social Network Analysis of Self-Control, Homophily, and Adolescent Relationships. *Journal of Quantitative Criminology, 27*(3), 251-273.

Young, J. T. N., Rebellon, C. J., Barnes, J. C., & Weerman, F. M. (2014). Unpacking the Black Box of Peer Similarity in Deviance: Understanding the Mechanisms Linking Personal Behavior, Peer Behavior, and Perceptions. *Criminology, 52*(1), 60-86.

Young, J. T. N., & Rees, C. (2013). Social Networks and Delinquency in Adolescence: Implications for Life-Course Criminology. In C. L. Gibson & M. D. Krohn (Eds.), *Handbook of Life-Course Criminology: Emerging Trends and Directions for Future Research* (pp. 159-180). New York, NY: Springer New York.

Young, R., Zhang, L., & Prybutok, V. R. (2007). Hacking into the Minds of Hackers. *Information Systems Management, 24*(4), 281-287.

Zhang, Y. P., Xiao, Y., Ghaboosi, K., Zhang, J. Y., & Deng, H. M. (2012). A Survey of Cyber Crimes. *Security and Communication Networks, 5*(4), 422-437.

Appendix: full cross-sectional survey (translated from Dutch)

Page 1

Welcome to the questionnaire of the "NL-ONLINE-OFFLINE" study.
Thank you for participating.

The questions are about your background and personal characteristics, your knowledge on computers and the internet and situations in which you encountered unsafe online or offline situations or rule-breaking behaviour or others or yourself. We would like to emphasise that this is a study or the university and it is carried out for scientific purposes only. Your information will not be shared. Your information will be treated confidentially, processed anonymously and stored safely. Your credentials will not be stored on the same place as your answers. You have been invited to participate in this study because you have ever been a possible subject in a judicial investigation. You can always reopen the questionnaire and start where you ended it. You can use the token you received for this. The questionnaire works most properly if java-script is enabled in your browser.

Note, to make sure that you are eligible for the ***50 euro voucher*** *it is important that you finish the questionnaire within 24 hours. At the end or the questionnaire, you can indicate which or the following vouchers you would like to receive: Bol.com, VVV-voucher or Zalando.*

Please read the statement below. If you agree, please thick the box and press Next at the bottom of the page.

Hereby I declare that I'm willing to participate in the study "NL-ONLINE-OFFLINE" on the background characteristics of persons, their computer- and internet knowledge and their experiences with unsafe online or offline situations and crime.
The researchers provided me with information on the contents, method and goals of the study. I had the opportunity to ask questions. I understand what the study is about. I understand that there will be questions on possible undesirable or rule-breaking behaviour of others or myself. I understand that my answers are confidential and can only be used for scientific purposes.

I take part in this study voluntarily. I have had enough time to decide if I want to participate. I understand that I can always stop participating if I don't want to any more.

I understand that I can always ask my questions to the study coordinator, Marleen Weulen Kranenbarg through e-mail (NL-ONLINE-OFFLINE@NSCR.NL) or between 9:00-17:00 by phone using 06-10846644.

□ Hereby I declare that I agree with the statement above and that I have read it completely.

Download/print this information

Page 2

1. What is your gender?

○ Male
○ Female

2. What is your year of birth?

___

3. In which country were you born?

○ Netherlands
○ Suriname
○ Netherlands Antilles or Aruba
○ Turkey
○ Morocco
○ Other, namely __________

4. In which country was your father born?

○ Netherlands
○ Suriname
○ Netherlands Antilles or Aruba
○ Turkey
○ Morocco
○ I don’t know
○ Other, namely __________

5. In which country was your mother born?

○ Netherlands
○ Suriname
○ Netherlands Antilles or Aruba
○ Turkey
○ Morocco
○ I don’t know
○ Other, namely __________

Note, as soon as you click the Next button you cannot go back to change your answers.

Page 3

6. What is your marital status at this moment?

○ Single
○ Living together
○ Married / registered partnership
○ Divorced
○ Widow / widower
○ I don't know

7. How many kids do you have?

(enter 0 if you don't have any kids)

___

8. What is your current housing situation?

(if you are sharing a house with peers please indicate that you are living alone)

(more than one answer possible)

I live…

□ … alone
□ … with my partner
□ … with my child/children
□ … with my parent/parents
□ … with other family
□ … with others
□ Other, namely __________

Page 4

9. Could you indicate below how many hours, apart from the hours you sleep, you spend on the following activities in a random week?

For instance: if you go for a 1 hour run 3 times a week you do that 3 hours a week. You should check the box of doing sports 1-5 hours a week.

If you always run with a friend you should also include these 3 hours in the hours you spend with friends somewhere else.

	In a random week I do this:					
	0 hours	**1-5 hours**	**6-10 hours**	**11-20 hours**	**21 hours or more**	**I don't want to answer**
Being at home alone	0	0	0	0	0	0
Being at home with family and/or my partner	0	0	0	0	0	0
Being at home with friends or acquaintances	0	0	0	0	0	0
Being at the home of my friends	0	0	0	0	0	0
Being somewhere else with friends	0	0	0	0	0	0
Being at work	0	0	0	0	0	0
Being at school	0	0	0	0	0	0
Studying	0	0	0	0	0	0
Doing sports	0	0	0	0	0	0
Going out (e.g. pub, club, restaurant, movies, etc.)	0	0	0	0	0	0

10. How often do you do the following things?

	Never	**Less than once a month**	**Once or a few times a month**	**Once or a few times a week**	**(almost) every day**	**I don't want to answer**
How often do you drink alcohol?	0	0	0	0	0	0
How often does it happen that you cannot control yourself because you had too much alcohol?	0	0	0	0	0	0
How often do you smoke weed or hashish?	0	0	0	0	0	0
How often do you use other drugs, like XTC, cocaine or something else?	0	0	0	0	0	0

Page 5

11. What kind of education are you following at this moment?

○ None
○ Primary school (or elementary school)
○ VMBO (lower secondary education)
○ HAVO, VWO, athenaeum, gymnasium (middle or upper secondary education)
○ MBO (lower tertiary education)
○ HBO (middle tertiary education)
○ University (higher tertiary education/university)
○ Other, namely __________

Are you not following education? Please enter None.

12. What is your highest completed education (education you have fully completed and for which you received a diploma or certificate)?

○ Primary school (or elementary school), VGLO, special education (primary education)
○ VMBO, MAVO, LBO, huishoudschool, VBO, LTS, ULO, MULO (lower secondary education)
○ HAVO, VWO, athenaeum, gymnasium, MMS, HBS (middle or upper secondary education)
○ MBO, leerlingwezen (BOL, BBL) (lower tertiary education)
○ HBO (middle tertiary education)
○ University (higher tertiary education/university)
○ I did not complete any education
○ I don't know
○ Other, namely __________

Page 6

[if the respondent was currently following education, the following question was asked]

13. Which of the educational fields below describes the best the education you are following at this moment?

○ General education
○ Economy, business and technology
○ Care, well-being, society, cultural and education
○ Informatics and ICT
○ I don't know

General education: *like primary school, general secondary school, education in personal skills etc.*

Economy, business and technology: *like hospitality, tourism, economics, administration, business, marketing, math, physics, engineering, etc.*

Care, well-being, society, cultural and education: *like medicine, nursing, social services, agriculture, psychology, journalism, law, music and arts education, (foreign) languages, history, pedagogy, etc.*

Informatics and ICT: *like IT, system and network management, artificial intelligence, and computer programming, etc.*

[if the respondent completed an education, the following question was asked]

14. Which of the educational fields below describe your highest education the best?

○ General education
○ Economy, business and technology
○ Care, well-being, society, cultural and education
○ Informatics and ICT
○ I don't know

General education: *like primary school, general secondary school, education in personal skills etc.*

Economy, business and technology: *like hospitality, tourism, economics, administration, business, marketing, math, physics, engineering, etc.*

Care, well-being, society, cultural and education: *like medicine, nursing, social services, agriculture, psychology, journalism, law, music and arts education, (foreign) languages, history, pedagogy, etc.*

Informatics and ICT: *like IT, system and network management, artificial intelligence, and computer programming, etc.*

Page 7

[if the respondent lived alone or indicated to live in an ‘other’ household, the questions below were asked]

15. In the past twelve months, what were your most important earnings?
(more than one answer possible)

□ I did not have any own earnings
□ Earnings from declared work
□ Earnings from undeclared work
□ Earnings from illegal activities
□ Earnings from benefits
□ Student financing
□ Pension
□ Received money from others
□ Savings, capital, other earnings
□ I don’t know
□ I don’t want to answer

[if the respondent indicated to have earnings, the following question was asked]

16. Of all earnings above, could you indicate what your overall mean net income (after tax) is per **month**?

○ up to a 1.000 euros a month
○ 1.000 - 2.000 euros a month
○ 2.000 - 3.000 euros a month
○ 3.000 - 4.000 euros a month
○ 4.000 - 5.000 euros a month
○ 5.000 euros or more a month
○ I don’t know
○ I don’t want to answer

17. Could you indicate if the next situations occurred in the past 12 months?
I have…

	Yes	No	I don’t want to answer
… saved money	0	0	0
… had just enough money to live	0	0	0
… had problems with making ends meet	0	0	0
… not been able to replace broken stuff	0	0	0
… had to borrow money for necessary expenses	0	0	0
… pledged belongings	0	0	0
… had creditors / bailiffs at my door	0	0	0
… had debts* of 5.000 euros or more	0	0	0

* These are all debts **except for mortgage or student loans.**

Page 7

[if the respondent indicated to live with others, the following questions were asked]

18. In the past twelve months, what were the most important earnings of your household?

(more than one answer possible)

□ My household did not have any own earnings
□ Earnings from declared work
□ Earnings from undeclared work
□ Earnings from illegal activities
□ Earnings from benefits
□ Student financing
□ Pension
□ Received money from others
□ Savings, capital, other earnings
□ I don't know
□ I don't want to answer

We mean the earnings of all people that you were living together with.

[if the respondent indicated to have earnings, the following question was asked]

19. Of all earnings above, could you indicate what your household's overall mean net income (after tax) is **per month**?

○ up to a 1.000 euros a month
○ 1.000 - 2.000 euros a month
○ 2.000 - 3.000 euros a month
○ 3.000 - 4.000 euros a month
○ 4.000 - 5.000 euros a month
○ 5.000 euros or more a month
○ I don't know
○ I don't want to answer

We mean the sum of all earnings of all people that were living in your household.

20. Could you indicate if the next situations occurred in your household in the past 12 months?

We have…

	Yes	No	I don’t want to answer
… saved money	0	0	0
… had just enough money to live	0	0	0
… had problems with making ends meet	0	0	0
… not been able to replace broken stuff	0	0	0
… had to borrow money for necessary expenses	0	0	0
… pledged belongings	0	0	0
… had creditors / bailiffs at my door	0	0	0
… had debts* of 5.000 euros or more	0	0	0

***** These are all debts **except for mortgage or student loans.**

Page 8

21. *The next seven pages contain statements. Some of these statements are in line with how you usually are. Others are not. We ask you to read these statements carefully and indicate to what extent these statements are true.*

Please select the applicable answer to every statement:

	Totally disagree	**Disagree**	**Don't agree, don't disagree**	**Agree**	**Totally agree**
I can look at a painting for a long time.	0	0	0	0	0
I neatly put away my clothes.	0	0	0	0	0
I remain unfriendly to someone who was mean to me.	0	0	0	0	0
People like me.	0	0	0	0	0
I avoid situations in which I can get injured.	0	0	0	0	0
I sometimes pretend to be better than I really am.	0	0	0	0	0
I like to read about new scientific discoveries.	0	0	0	0	0
I work harder than others.	0	0	0	0	0
I often express criticism.	0	0	0	0	0
I stay in the background when I'm in a group.	0	0	0	0	0
I worry about unimportant things.	0	0	0	0	0
I wouldn't say anything if I were charged too little.	0	0	0	0	0
I have a lot of imagination.	0	0	0	0	0
I typically check my work carefully.	0	0	0	0	0
I often change my opinions to match those of others.	0	0	0	0	0

Page 9

Please select the applicable answer to every statement:

	Totally disagree	Disagree	Don't agree, don't disagree	Agree	Totally agree
I prefer to work alone rather than with others.	0	0	0	0	0
I can deal with personal problems all by myself.	0	0	0	0	0
I want others to see how important I am.	0	0	0	0	0
I like people with strange ideas.	0	0	0	0	0
I think carefully before I do something unsafe.	0	0	0	0	0
I sometimes react very strongly when faced with a setback.	0	0	0	0	0
I have a lust for life.	0	0	0	0	0
I strongly feel others' pain.	0	0	0	0	0
I am an ordinary person; anything but special.	0	0	0	0	0
I find most art dull.	0	0	0	0	0
I have a tough time finding things because I'm untidy.	0	0	0	0	0
I quickly trust others again after they have cheated on me.	0	0	0	0	0
Nobody likes me.	0	0	0	0	0
I can easily withstand physical pain.	0	0	0	0	0
I sometimes tell lies to get my way.	0	0	0	0	0

Page 10

Please select the applicable answer to every statement:

	Totally disagree	Disagree	Don't agree, don't disagree	Agree	Totally agree
I think science is boring.	0	0	0	0	0
If something is hard, I give up easily.	0	0	0	0	0
I am gentle to others.	0	0	0	0	0
I easily approach strangers.	0	0	0	0	0
I often worry that something will go wrong.	0	0	0	0	0
I am curious about how you can earn a lot of money in a dishonest way.	0	0	0	0	0
I love thinking up new ways of doing things.	0	0	0	0	0
I think it's a waste of time to check my work for errors.	0	0	0	0	0
I easily give in to others.	0	0	0	0	0
I prefer being on my own.	0	0	0	0	0
I rarely need support from others.	0	0	0	0	0
I want to own valuable things.	0	0	0	0	0
It would bother me if people thought I was strange.	0	0	0	0	0
I generally do whatever comes to mind.	0	0	0	0	0
I am rarely angry at someone.	0	0	0	0	0

Page 11

Please select the applicable answer to every statement:

	Totally disagree	Disagree	Don't agree, don't disagree	Agree	Totally agree
I am often in a sombre mood.	0	0	0	0	0
I sometimes feel tears welling up when I tell someone goodbye.	0	0	0	0	0
I wouldn't want people to treat me like I'm better than them.	0	0	0	0	0
I love poetry.	0	0	0	0	0
My bedroom is always tidy.	0	0	0	0	0
I stay wary of people who have wronged me.	0	0	0	0	0
Nobody likes talking with me.	0	0	0	0	0
I am afraid of feeling pain.	0	0	0	0	0
I'm bad at putting on an act around other people.	0	0	0	0	0
Nature programs on television bore me.	0	0	0	0	0
I postpone complicated tasks as long as possible.	0	0	0	0	0
I react negatively to people who make mistakes.	0	0	0	0	0
I often act as the spokesperson when I'm in a group.	0	0	0	0	0
I worry less than others.	0	0	0	0	0
I wouldn't cheat on anyone, not even if that person was an idiot	0	0	0	0	0

Page 12

Please select the applicable answer to every statement:

	Totally disagree	Disagree	Don't agree, don't disagree	Agree	Totally agree
I love making unusual things.	0	0	0	0	0
I work very precisely.	0	0	0	0	0
Others have a hard time changing my ideas.	0	0	0	0	0
I like having a lot of people around me.	0	0	0	0	0
I need others to comfort me.	0	0	0	0	0
I wear beat up rather than expensive clothes.	0	0	0	0	0
Others think I have strange ideas.	0	0	0	0	0
I tend to control myself well.	0	0	0	0	0
Even when I'm treated badly, I remain calm.	0	0	0	0	0
I am generally cheerful.	0	0	0	0	0
I get sad when a good friend leaves for a long time.	0	0	0	0	0
I'm special and superior in many ways	0	0	0	0	0
It amazes me that people want to spend money on art.	0	0	0	0	0
I make sure that things are in the right spot.	0	0	0	0	0
I am a very trusting person.	0	0	0	0	0

Page 13

Please select the applicable answer to every statement:

	Totally disagree	Disagree	Don't agree, don't disagree	Agree	Totally agree
I get the feeling many people dislike me.	0	0	0	0	0
I am more daring than others in dangerous situations.	0	0	0	0	0
I find it difficult to lie.	0	0	0	0	0
I would enjoy reading a book about inventions.	0	0	0	0	0
I'd rather take it easy than work hard.	0	0	0	0	0
I immediately show it if I find something stupid.	0	0	0	0	0
I feel uncomfortable in an unfamiliar group.	0	0	0	0	0
Even under stress, I sleep well.	0	0	0	0	0
If I damaged something when nobody was around, I'd keep it to myself.	0	0	0	0	0
My work is often original.	0	0	0	0	0
I always re-read what I write to make sure that it is error-free.	0	0	0	0	0
I tend to quickly agree with others.	0	0	0	0	0
I like to talk with others.	0	0	0	0	0
I can easily overcome difficulties on my own.	0	0	0	0	0
I want to be famous.	0	0	0	0	0

Page 14

Please select the applicable answer to every statement:

	Totally disagree	Disagree	Don't agree, don't disagree	Agree	Totally agree
People are surprised by the beliefs I have.	0	0	0	0	0
I often do things without really thinking.	0	0	0	0	0
People have seen me get into in a rage.	0	0	0	0	0
I am seldom cheerful.	0	0	0	0	0
I have to cry during sad or romantic movies.	0	0	0	0	0
I am entitled to special treatment.	0	0	0	0	0

Page 15

Next are questions on your use of computers, ICT-systems and the internet.

22. Could you indicate below how many hours you spend on the following (digital) activities in a random week? *(During both your leisure time and possibly during your work)*

	In a random week I do this:					
	0 hours	1-5 hours	6-10 hours	11-20 hours	21 hours or more	I don't want to answer
E-mailing, chatting online or using social media (like Facebook, Twitter etc.)	0	0	0	0	0	0
Surfing on the internet	0	0	0	0	0	0
Online shopping	0	0	0	0	0	0
Gaming	0	0	0	0	0	0
Reading internet forums and/or posting messages on these forums	0	0	0	0	0	0
Creation and maintenance of websites	0	0	0	0	0	0
Illegal downloading	0	0	0	0	0	0
Programming	0	0	0	0	0	0

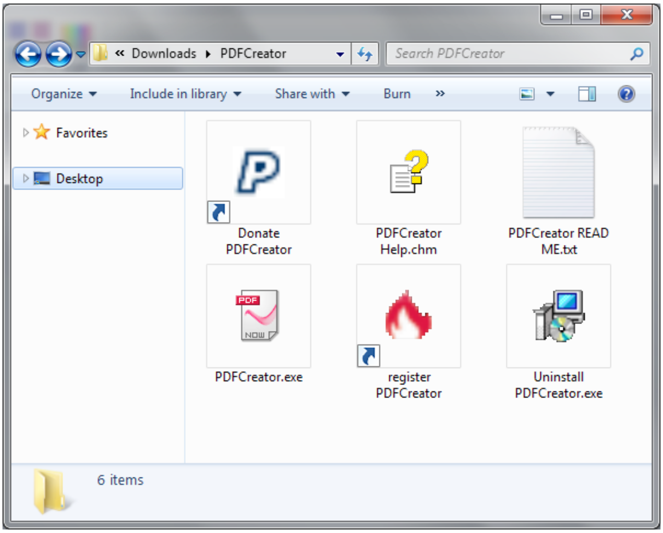
23. Could you indicate which of the following statements is most applicable to you?

○ I don't like using computers and don't use them unless I absolutely have to
○ I can surf the net, use some common software but not fix my own computer
○ I can use a variety of software and fix some computer problems I have
○ I can use Linux, most software, and fix most computer problems I have
○ I can use different programming languages and am capable of detecting programming errors

Page 16

The next questions are about your knowledge on computers, ICT-systems and the internet. It doesn't matter if you don't know the answer to a question, we are interested in your knowledge and therefore we ask you to answer ***without the help of others*** *and* ***without looking up the answers.*** *If you don't know the answer, you can check the 'I don't know' box.*

Page 17



24. You have downloaded the program PDFCreator and you want to use it right away.

You should double click on one of the icons above, which one?

○ PDFCreator Help.chm
○ PDFCreator READ ME.txt
○ PDFCreator.exe
○ Uninstall PDFCreator.exe
○ I don't know

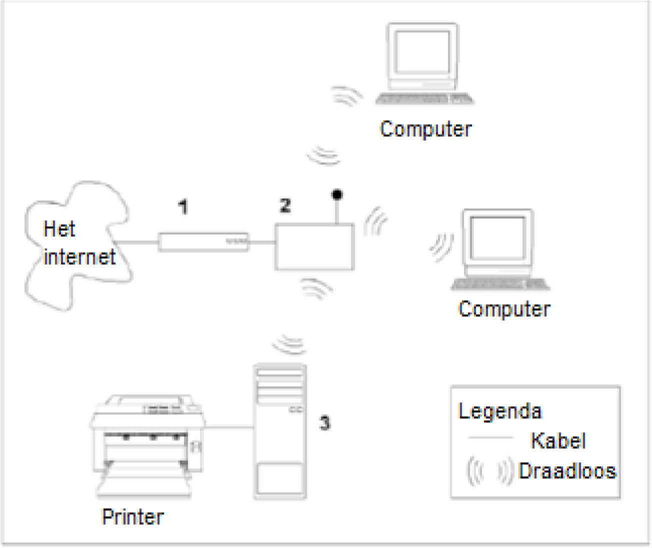
25. What encoding is most likely used in the string below and what does it say without encoding?

"YmFzZTY0IG5hdHVlcmxpamshCg=="

○ The encoding used is: base64
Without encoding is says: "base64 natuurlijk!"
○ The encoding used is: uuencoding
Without encoding is says: "uuencoding is gaaf"
○ The encoding used is: base64
Without encoding is says: "waarom geen base64?"
○ The encoding used is: yenc
Without encoding is says: "wordt usenet nog gebruikt?"
○ I don't know

Page 18

The picture below shows an office network:



26. Which of the following descriptions describe the devices most accurately?

○ Device 1 is a Broadband modem; Device 2 is a Wireless router; Device 3 is a Wireless printer server

○ Device 1 is a Wireless router; Device 2 is a Broadband modem; Device 3 is a network fileserver

○ Device 1 is a Network fileserver; Device 2 is a Hub; Device 3 is a Wireless printer server

○ Device 1 is a Broadband modem; Device 2 is a Wireless print server; Device 3 is a Wireless router

○ I don't know

27. In MySQL, where is de metadata saved?

○ In the MySQL database “mysql”

○ In the MySQL database “metadata”

○ In the MySQL database “metasql”

○ None of the answers above is correct

○ I don't know

Page 19

28. Which of the following email addresses can be valid?

○ www.infobedrijfx.nl
○ info@bedrijfx.nl
○ https://www.infobedrijfx.nl
○ info@bedrijfx
○ I don’t know

29. Below are statements, which of these statements is/are correct?

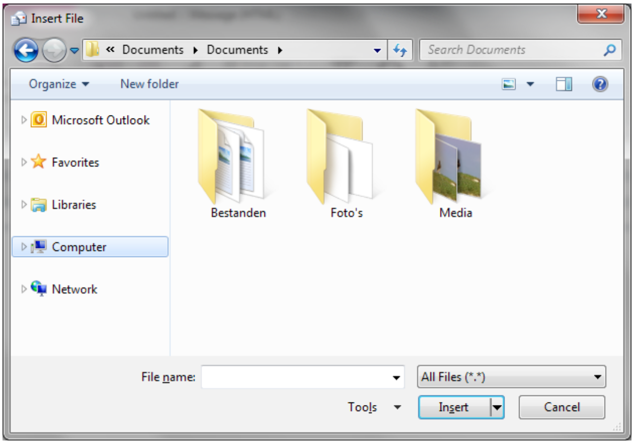
Statement 1: Virtual Machines are used for making the best use of available hardware

Statement 2: Virtual Machines are an easy way to separate different users

Statement 3: In a Virtual Machine you are protected against malware

○ statement 1 is correct
○ statement 2 is correct
○ statement 1 and 2 are correct
○ statement 2 and 3 are correct
○ I don’t know

Page 20



30. Imagine you want to attach the folders above to an e-mail.
What is the best way to do this?

○ Select all three folders and click on insert
○ Zip all folders to a '.zip' folder, select that folder and click on insert
○ Click on 'All Files' and select the file type 'folder', select all folders and click on insert
○ Open all folders, select all files in the folders and click on insert
○ I don't know

31. Which of the following websites uses encryption?

○ www.webshop.nl/secure
○ http://www.webshop.nl/secure
○ https://www.webshop.nl/secure
○ httpv://www.webshop.nl/secure
○ I don't know

Page 21

32. In what order are webpages loaded?

○ URL => IP => DNS

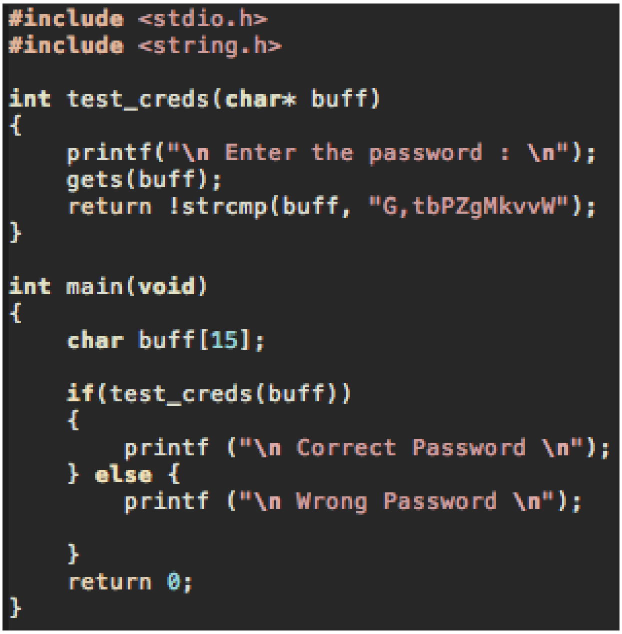
○ IP => DNS => URL

○ URL => DNS => IP

○ IP => URL => DNS

○ I don't know

In the code below it is possible to execute your own code.



```
#include <stdio.h>
#include <string.h>

int test_creds(char* buff)
{
    printf("\n Enter the password : \n");
    gets(buff);
    return !strcmp(buff, "G,tbPZgMkvvW");
}

int main(void)
{
    char buff[15];

    if(test_creds(buff))
    {
        printf ("\n Correct Password \n");
    } else {
        printf ("\n Wrong Password \n");

    }
    return 0;
}
```

33. Which of the techniques below is not suitable to hinder and/or prevent this kind of misuse?

○ PaX

○ Taint checking

○ SEH

○ ASLR

○ I don't know

Page 22

34. Could you indicate from which of the sources below you gained your knowledge and skills on computers, ICT-systems and the internet?

I have my knowledge and skills about computers, ICT-systems and the internet from ...

	Completely false	False	Not true, not false	True	Totally true
... books or magazines	0	0	0	0	0
... television or movies	0	0	0	0	0
... websites	0	0	0	0	0
... short online videos or movies (for instance on YouTube etc.)	0	0	0	0	0
... online forums	0	0	0	0	0
... school, study or a course	0	0	0	0	0
... trying it myself	0	0	0	0	0
... conversations with others	0	0	0	0	0
... meetings about these subjects	0	0	0	0	0
... watching others who are doing it	0	0	0	0	0

Page 23

The next questions are about your experiences with online (digital) crime in the past twelve months.

35. How often **in the past twelve months...**

	0 times	1 time	2 times	3-5 times	6-10 times	More often	I don't want to answer
… did malware (malicious software) damage your computer and/or the files on your computer?	o	o	o	o	o	o	o
… did somebody break in or logged on to your computer, website, network, online profile (like Facebook) or another account without your permission?	o	o	o	o	o	o	o
… did somebody steal, change, damage or capture digital information or computer files from you?	o	o	o	o	o	o	o
… did somebody change the content of you website or online profile (like Facebook, Twitter) without your permission?	o	o	o	o	o	o	o
… did somebody blocked to access to your website?	o	o	o	o	o	o	o
… did you click on a link in a phishing email* or you provided your credentials through a phishing email?	o	o	o	o	o	o	o

* A phishing email is an email of which the sender pretends to be someone else, you bank for instance, in an effort to steal you bank credentials or let you click on a link.

36. Aside from the incidents above, have you been victim of another online (digital) crime **in the past twelve months?**

○ Yes, namely __________

○ No

Page 24

The next questions are about your experiences with _offline (non-digital)_ *crime in the past twelve months.*

37. How often **in the past twelve months...**

	0 times	1 time	2 times	3-5 times	6-10 times	More often	I don't want to answer
… did somebody try to break into you house without stealing anything?	0	0	0	0	0	0	0
… has something been stolen from your home?	0	0	0	0	0	0	0
… has your bicycle or a bicycle of your household been stolen?	0	0	0	0	0	0	0
… has something else, aside from the thefts already mentioned, been stolen from you?	0	0	0	0	0	0	0
… did somebody break or damage something of you, without stealing something from you?	0	0	0	0	0	0	0
… did somebody threaten to hit you, to kick you, with a gun, a knife or something else, without you being attacked or assaulted?	0	0	0	0	0	0	0
… did somebody attacked or assaulted you by hitting or kicking you or by using a gun, knife or something else against you?	0	0	0	0	0	0	0
… did somebody assault you sexually?	0	0	0	0	0	0	0

38. Aside from the incidents above, have you been victim of another offline (non-digital) crime **in the past twelve months?**

○ Yes, namely __________

○ No

Page 25

Many people sometimes do things that are not allowed or that are against the law. The following questions are about online (digital) activities you might have done. Please answer as honest as possible.

39. ***In the past twelve months****, how often did you ...* ***without permission***

	0 times	1 time	2 times	3-5 times	6-10 times	More often	I don't want to answer
… make available an illegal copy of computer software, music or movies etc. to others?	0	0	0	0	0	0	0
… break in or log on to a network, computer or web account by guessing the password?	0	0	0	0	0	0	0
… gain access to a network, computer, web account or files that were saved on that in another way?	0	0	0	0	0	0	0
… sell or give credentials of somebody else to someone?	0	0	0	0	0	0	0
… remove, add or change something to the computer files of somebody else?	0	0	0	0	0	0	0
… copy information saved on a network, computer or web account?	0	0	0	0	0	0	0
… sell or give information or files of somebody else to someone?	0	0	0	0	0	0	0

Page 26

40. ***In the past twelve months****, how often did you …* ***without permission***

	0 times	1 time	2 times	3-5 times	6-10 times	More often	I don't want to answer
… used or distributed a computer program that could harm a network, computer etc. (like a virus, worm)?	0	0	0	0	0	0	0
… take over the control on a network, computer or web account?	0	0	0	0	0	0	0
… change the contents of a webpage or online profile (like Facebook, Twitter)?	0	0	0	0	0	0	0
… modify, monitor or misuse in another way the communication between a user and a webpage?	0	0	0	0	0	0	0
… try to take down a website by providing it with large amounts of data?	0	0	0	0	0	0	0
… try to gain someone else's credentials by pretending to be someone else?	0	0	0	0	0	0	0
… send large amounts of emails that were meant to deceive others?	0	0	0	0	0	0	0

Page 27

There are also offline things that are not allowed or are against the law, but many people sometimes do. The following questions are about offline (non-digital) activities you might have done. Please answer as honest as possible

41. In the past twelve months, how often ...

	0 times	1 time	2 times	3-5 times	6-10 times	More often	I don't want to answer
… did you travel on purpose without a valid ticket by public transport (tram, bus, train or metro), that is to say fare dodging?	0	0	0	0	0	0	0
… did you steal something worth more than five euros (from a person, on the street, from a house, from a store, at work, etc.)?	0	0	0	0	0	0	0
… commit a burglary (in a house, building, store, office, car, etc.)?	0	0	0	0	0	0	0
… did you buy or sell something worth more than 10 euros while you knew or expected that is was stolen?	0	0	0	0	0	0	0
… did you conceal or incorrectly declare money you earned to the tax authorities on purpose?	0	0	0	0	0	0	0
… did you intentionally declare something incorrect to an insurance company (for instance travel or household insurance)?	0	0	0	0	0	0	0
… did you intentionally damaged or daubed something like a traffic sign, a window, a car, a building or something else?	0	0	0	0	0	0	0

Page 28

42. In the past twelve months, how often …

	0 times	1 time	2 times	3-5 times	6-10 times	More often	I don’t want to answer
… did you drive a car while you drank more than permitted?	0	0	0	0	0	0	0
… did you threaten someone (directly, trough phone, email, etc.) to scare, rob or control that person?	0	0	0	0	0	0	0
… did you carry a weapon to use or protect yourself?	0	0	0	0	0	0	0
… did you hit or kicked someone during which that person was wounded?	0	0	0	0	0	0	0
… did you wound someone with a weapon?	0	0	0	0	0	0	0
… did you force someone into sexual activities?	0	0	0	0	0	0	0
… did you set something on fire (like a building, house, car, etc.)?	0	0	0	0	0	0	0

Page 29-57

[for each crime that a respondent reported to have committed at least once, the following two questions were asked]
[a short description of the crime that was reported was inserted below, indicated by the text [**short description**]]

43. *You indicated that you ever* [**short description**]. *The last time you did this, could you indicate which of the following reasons for doing that were applicable?*

I did it …

	Totally disagree	Disagree	Don't agree, don't disagree	Agree	Totally agree
… to earn something with it	0	0	0	0	0
… to damage something	0	0	0	0	0
… because of boredom, curiosity or excitement	0	0	0	0	0
… because it was fun and/or felt good	0	0	0	0	0
… because it was challenging and/or educational	0	0	0	0	0
… for revenge, because of anger or to bully someone	0	0	0	0	0
… to put things straight and/or to deliver a message	0	0	0	0	0
… to impress others or to gain power	0	0	0	0	0
… to see how far I could go	0	0	0	0	0

44. Did you do it together with one or more others?
(more than one answer possible)

□ Yes, with one or more of my friends
□ Yes, with one or more of my family members
□ Yes, with one or more others
□ No, I did it on my own
□ I don't want to answer

<u>Page 58</u>

We are also interested in the contacts people have with others. The following questions are about the contacts you had with others in the past 12 months.

45. *Everybody needs somebody to discuss important things with. With whom did you discuss important things <u>in the past 12 months</u>? Fill in a name or nickname below, which you could use to identify this person. U can use a fake name, as long as you know who it is. Choose the most important persons, you can enter up to five names.*

Name 1: __________
Name 2: __________
Name 3: __________
Name 4: __________
Name 5: __________

□ Not applicable, I did not discuss important things with other during the past twelve months

□ I don't want to answer

Page 59

[the questions on the following pages were only asked if the respondent provided at least one name of a social network member on the previous page]
[on the following pages, the name the respondent provided was inserted as indicated by [name 1-5]]

46. What is your relationship with this person?

	My partner	My child	My father/ mother	My brother/ sister	Other family	A friend	I don't want to answer
[name 1]	0	0	0	0	0	0	0
[name 2]	0	0	0	0	0	0	0
[name 3]	0	0	0	0	0	0	0
[name 4]	0	0	0	0	0	0	0
[name 5]	0	0	0	0	0	0	0

47. What is this person's gender?

	Male	Female	I don't know	I don't want to answer
[name 1]	0	0	0	0
[name 2]	0	0	0	0
[name 3]	0	0	0	0
[name 4]	0	0	0	0
[name 5]	0	0	0	0

48. What age is this person approximately?

(If you don't know the age exactly please indicate how old you think this person is)

[name 1] is __________

[name 2] is __________

[name 3] is __________

[name 4] is __________

[name 5] is __________

Page 60

49. How often do you have contact with this person through online text messages (like email, chat, forums, social media, WhatsApp etc.)?

	Daily	Several times a week	Once a week	Once a month	Once every three months	Less than once every three months	I don't want to answer
[name 1]	0	0	0	0	0	0	0
[name 2]	0	0	0	0	0	0	0
[name 3]	0	0	0	0	0	0	0
[name 4]	0	0	0	0	0	0	0
[name 5]	0	0	0	0	0	0	0

50. How often do you speak to this person in both an online or offline phone call (like by phone or Skype etc.)?

	Daily	Several times a week	Once a week	Once a month	Once every three months	Less than once every three months	I don't want to answer
[name 1]	0	0	0	0	0	0	0
[name 2]	0	0	0	0	0	0	0
[name 3]	0	0	0	0	0	0	0
[name 4]	0	0	0	0	0	0	0
[name 5]	0	0	0	0	0	0	0

51. How often do you see this person offline (not on the internet, but in real life)?

	Daily	Several times a week	Once a week	Once a month	Once every three months	Less than once every three months	I don't want to answer
[name 1]	0	0	0	0	0	0	0
[name 2]	0	0	0	0	0	0	0
[name 3]	0	0	0	0	0	0	0
[name 4]	0	0	0	0	0	0	0
[name 5]	0	0	0	0	0	0	0

Page 61

52. In general, what does this person think about committing online (digital) criminal offences?

(like without permission breaking into a computer/network/account, misusing data on ICT systems, digital attacks on sites or companies, without permission changing digital information of somebody else, etc.)

This person

	Mostly approves it	Sometimes approves sometimes disapproves it	Always disapproves it	I don't know
[name 1]	0	0	0	0
[name 2]	0	0	0	0
[name 3]	0	0	0	0
[name 4]	0	0	0	0
[name 5]	0	0	0	0

53. In general, what does this person think about committing offline (non-digital) criminal offences?

(like stealing money or goods, committing fraud, vandalism, threatening, using violence, etc.)

This person

	Mostly approves it	Sometimes approves sometimes disapproves it	Always disapproves it	I don't know
[name 1]	0	0	0	0
[name 2]	0	0	0	0
[name 3]	0	0	0	0
[name 4]	0	0	0	0
[name 5]	0	0	0	0

Page 62

54. As far as you know, did this person commit online (digital) criminal offences in the past 12 months?

(like without permission breaking into a computer/network/account, misusing data on ICT systems, digital attacks on sites or companies, without permission changing digital information of somebody else, etc.)

	Yes	No	I don't want to answer
[name 1]	0	0	0
[name 2]	0	0	0
[name 3]	0	0	0
[name 4]	0	0	0
[name 5]	0	0	0

55. As far as you know, did this person commit offline (non-digital) criminal offences in the past 12 months?

(like stealing money or goods, committing fraud, vandalism, threatening, using violence, etc.)

	Yes	No	I don't want to answer
[name 1]	0	0	0
[name 2]	0	0	0
[name 3]	0	0	0
[name 4]	0	0	0
[name 5]	0	0	0

Page 63

56. *We want to make sure that you have taken the time to read all the questions. If you did not, some of your answers cannot be used. To check whether you have read this, we ask you to select the option, 'Other, namely ...' and fill in 'gelezen'. Thank you for your cooperation.*

□ Soccer

□ Volleyball

□ Basketball

□ Hockey

□ Martial arts (like judo, boxing)

□ Swimming

□ Fitness or strength training

□ I don't do any sports

□ Other, namely __________

Page 64

You are almost at the end of the questionnaire.

57. Could we contact you for further research in the future?

○ Yes

○ No

For scientific research it is relevant to link the answers you just provided us with to information that is known about you in local or national databases (like the Sociaal Statistisch Bestand and the Justitieel Documentatie Systeem). This will only be done if you give us permission to do so. This information will, of course, also be treated confidentially, processed anonymously and stored safely. If you have any questions about this you can always contact the coordinator of this study, Marleen Weulen Kranenbarg by email (NL-ONLINE-OFFLINE@NSCR.NL) or between 9:00-17:00 by phone on 06-10846644.

Download/print this information

58. Do you give your permission?

○ Yes, I hereby declare that I give permission to link my answers to information that is known about me in local or national databases.

○ No, I hereby declare that I do not give permission to link my answers to information that is known about me in local or national databases.

Page 65

[this page was only shown if the respondent indicated that we could contact him or her for future research]

59. You indicated that we could contact you for future research. Could you, if you want to, provide us with your phone number (landline and/or mobile) and/or your email address so that we can easily get in touch with you?

The information provided on this page will only be used to contact you and will not be stored in the same place as your answers to the questionnaire. If you have any questions you can always contact the coordinator of this study, Marleen Weulen Kranenbarg by email (NL-ONLINE-OFFLINE@NSCR.NL) or between 9:00-17:00 by phone on 06-10846644.

Mobile phone number __________
For verification, once again your mobile phone number __________
Landline number __________
For verification, once again your landline number __________
Email address __________
For verification, once again your email address __________
□ For future research you can contact me by sending a letter

Page 66

Thank you for your participation, you completed the questionnaire!

To thank you for your participation you will receive a 50-euro voucher. The information provided on this page will only be used to send you the voucher and will not be stored in the same place as your answers to the questionnaire. If you have any questions you can always contact the coordinator of this study, Marleen Weulen Kranenbarg by email (NL-ONLINE-OFFLINE@NSCR.NL) or between 9:00-17:00 by phone on 06-10846644.

*Note! It is important that you complete the information on this and the following pages, only then we will be able to send you the voucher. We will start sending the vouchers on **July 27th 2015.***

Download/print this information

60. How do you want to receive your voucher?

○ By mail, at the same address I received the invitation letter for this study.
○ By mail, at another address.
○ I don’t want to receive a voucher.

Page 67

[if the respondent indicated that he or she wanted to receive a voucher, the following question was asked]

Note! It is important that you complete the questions on this page and click on send at the bottom of the page, only then we will be able to send you the voucher.

61. Select which voucher you wish to receive.

○ Bol.com

○ VVV-bon

○ Zalando

[if the respondent indicated that he or she wanted to receive the voucher at a different address, the following question was asked]

62. *You have indicated that you want us to send the voucher to a different address than the address you received the invitation letter for this study at.*

Enter the address below.
Note, make sure the address is complete and correct.

Street name __________
Number (including a possible addition like 1, 1A, 1 Bis, etc.) __________
Postal code (for instance 1234AB) __________
City __________

63. If you have any remarks, please write them below

____
____
____
____
____
____
____
____

As soon as you click the send button below your information on the voucher will be send.

English summary

Cyber-offenders versus traditional offenders: An empirical comparison

The main goal of this dissertation was to empirically compare cyber-offenders with traditional offenders on four domains in criminology: offending over the life-course, personal and situational risk factors for offending and victimisation, similarity in deviance in the social network, and motivations related to different offence clusters. The focus was on new forms of crime that target IT and in which IT is key in the commission of the crime, so-called cyber-dependent crimes, like malicious hacking, web defacement, illegal control over IT-systems, malware use, and so on. These crimes provide a unique test case for traditional criminological explanations for offending, as these did not exist prior to the rise in the use of IT-systems. The anonymous digital context in which these crimes take place may have changed, for example, the situations in which opportunities for committing crime occur, the skills and personality characteristics that are needed to commit these crimes, the perceptions of the consequences of offending, and the interpersonal dynamics between offenders and victims.

Results

Offending over the life-course

In Chapter 2, a longitudinal dataset of registration data for the period 2000-2012 was used to study cyber-offending and traditional offending over the life-course. The results seem to indicate that social control of others can reduce the likelihood of cyber-offending. Nevertheless, some traditionally protective life circumstances can increase opportunities for cyber-offending and apparently the control of others in these situations cannot prevent a person from using those opportunities to commit cybercrime.

For personal life circumstances it was found that living with a partner or with a partner and a child reduces the likelihood of cyber-offending, and living as a single parent increases the likelihood of offending, in comparison to living alone. These estimates were in the same direction and even stronger for cybercrime compared to traditional crime. With respect to professional life circumstances, there was no statistically significant effect of employment or enrolment in education on cyber-offending, while these life circumstances did reduce traditional offending statistically significantly. Within the complete offender population of this study, general employment reduced the likelihood of cyber-offending, but employment in the IT-sector and being enrolled in education increased the likelihood of cyber-offending (not statistically significant).

Risk factors for offending, victimisation, and victimisation-offending

Based on the cross-sectional dataset collected for this dissertation, Chapter 3 compared patterns in personal and situational risk factors for separate groups of offenders-only, victims-only and victim-offenders, between cybercrime and traditional crime. The results indicated the existence of a victim-offender overlap for cybercrime. For both cybercrime and traditional crime, victim-offenders had more risk factors. Differences between the two types of crime were mostly found in situational risk factors that seem to be the result of the different context in which these crimes take place. Online activities are more important for cybercrime, while offline activities are more important for traditional crime.

For cybercrime, offenders-only committed the relatively more technically sophisticated crimes compared to victim-offenders. This was also reflected in the risk factors for offenders-only, as the likelihood of offending-only was higher if a person had more IT-skills, did not have a statistically significantly low self-control, and had online activities in which they could increase their criminal IT-skills. For victim-offenders, on the other hand, IT-skills also increased the likelihood of victimisation-offending, but less so compared to offenders-only. In addition, low self-control increased the likelihood of victimisation-offending. Lastly, more general online routine activities, in which both opportunities for offending and risks for victimisation could emerge, were related to victimisation-offending.

Similarity in deviance of social network members

Based on ego-centred network data from the cross-sectional survey dataset collected for this dissertation, Chapter 4 compared the relation between deviance of an individual and deviance of a social network member between cybercrime and traditional crime. A statistically significant similarity in deviance was found for cybercrime, but the comparison with traditional crime indicated that this similarity was much weaker for cybercrime.

Subsequently, this chapter indicated that both for cybercrime and traditional crime the relation is stronger for daily-contacted network members of the same gender. However, for cybercrime the relation is strongest for older social network members, while for traditional crime the relation is strongest for same-aged contacts. This indicates that older role models may be relatively more important for cybercrime compared to traditional crime.

Clusters of offences and related motivations

Chapter 5 used the self-reported offending questions from the cross-sectional dataset to examine which clusters of crime could be identified and to what extent cyber-offenders could be distinguished from traditional offenders. The analyses indicated that cyber-dependent crime is seldom committed by offenders who also commit traditional crimes. The cybercrimes that were often committed by the same offender appeared to be part of the same modus operandi or to be related because they require the same skill set and context.

In addition, self-reported motivations were used to examine which motivations offenders provide for the different clusters of offending and to what extent the clusters can be distinguished from the others by these motivations. The cyber-offenders in this sample almost never indicated a financial motivation. Intrinsic motivations, like curiosity and learning from committing crimes, were most important for all cybercrime clusters. Extrinsic motivations were less important for cybercrime compared to traditional crime. However, some differences between the cybercrimes could be observed for extrinsic motivations, as hacking and internet related crimes were more often committed to put things straight or deliver a message, and internet related crimes were also more often committed out of revenge, anger or to bully someone. Impressing others or trying to gain power was rarely indicated as a motivation for cyber-offending.

Limitations

The samples in this dissertation were drawn from police and prosecutor's data. For Chapter 2, this means that it is unknown if a person was actually guilty of committing a crime and it is unknown to what extent this person also committed crimes in the years he or she was not caught by the police. For Chapter 3 to 5, this means that the analyses indicated which present-day risk factors, social contacts and motivations were related to present-day self-reported offending of people who had been caught by the police for committing a crime in the past, prior to the twelve-month period of the self-report questions. In addition, because of the dark number in police or prosecutor's data, these are selective samples. The results only reflect the people who have been caught for committing a crime.

For Chapter 2 the nature of the data limited the depth of the variables under study. For example, registration data cannot inform us about the strength of social bonds and people's actual daily activities. The data used in Chapter 3 to 5 provided more in-depth measures, but the cross-sectional nature of the data limited the ability to draw strong causal conclusions from the analyses. Lastly, the data used are based on Dutch adults. It is unknown to what extent the results also apply to juveniles and adolescents or offenders from other countries.

Future research

Replication in future research in different and larger samples, preferably with in-depth longitudinal data, is necessary. In-depth longitudinal research is necessary to (1) find the exact causal processes and life circumstances that lead to committing cybercrime or desistence from committing cybercrime, (2) identify processes of selection and influence in online and offline social networks for cybercrime, and (3) to examine a possibly causal relationship between offending and victimisation. In order to be able to use interventions that are based on explanations for traditional crime, it is necessary to keep studying the differences between cyber-offenders and traditional offenders.

Future research could examine to what extent selection and influence processes can be found in, for example, online forums and gaming communities. That research could also shed light on the extent to which these online social contacts and online interactions are comparable to traditional social contacts and offline interactions. In addition, longitudinal research on social networks and cybercrime should use a method in which all network members report on their own deviant behaviour. This will enhance our knowledge on (1) selection and influence processes, (2) the discrepancy between perceived and actual cyber-deviance of social contacts, (3) the extent to which actual and perceived deviance of social contacts differently influences cyber-offending, and (4) to what extent the invisibility of cyber-deviance results in a larger discrepancy for cybercrime compared to traditional crime.

In-depth qualitative interviews could provide us with more detailed information on, for example, the role of older social network members or the strategy that offenders use if they commit a cybercrime and if they actively seek opportunities for cyber-offending or if they simply come across these opportunities by chance during their daily activities. Future research could also focus on the role of IT-skills. For example, differences in the level of IT-skills needed to commit different types of cyber-dependent crime and in longitudinal research how people acquire IT-skills and knowledge on how to use those skills in an illegal manner over time.

Practical implications

It should be noted, that none of the prevention and intervention strategies discussed below have been evaluated empirically for cybercrime and recommendations are based on a limited number of empirical studies. Therefore, authorities that are responsible for designing and executing prevention and intervention programs, are advised to carefully design and implement evaluation studies of the programs they design for cybercrime. When using interventions designed for traditional offenders, empirically identified differences and similarities between cyber-offenders and traditional offenders should be kept in mind. It is not advisable to base the application of traditional interventions to cybercrime purely on hypothetical similarities.

Based on the comparisons in this dissertation it is to be expected that interventions for cybercrime may benefit from stimulating offenders to satisfy their IT-related curiosity in legitimate ways. One way of doing that may be to help them find employment in which they could use their skills. It is, however, important that cyber-offenders are offered ethical guidance in their path to a legitimate profession and both strong formal and informal social control should be established in their professional life. Another promising way of helping offenders to move to responsible use of IT is by assigning them to a mentor.

In interventions it could be useful that offenders who commit the more technical types of crime may behave more rational than other offenders and they may be able to assess the different ways in which they could act responsibly after they discover a vulnerability. Additionally, interventions that increase the perceived consequences for the offender and his or her victim may be helpful, for example with so-called 'cease and desist visits' or situational crime prevention.

Conclusion

The empirical research conducted on the four domains in this dissertation, indicated that correlates of cyber-offending are to some extent similar to correlates of traditional offending. Nevertheless, important differences occur in each domain, which seems to be the result of the different context in which cybercrime takes place. These differences should be kept in mind when applying explanations for traditional offending to cyber-offending. Predictions and measures based on those explanations should be adjusted to the digital domain and the strength of these predictors should be empirically compared between cybercrime and traditional crime.

Nederlandse samenvatting
(Dutch Summary)

Cyber-delinquenten versus traditionele delinquenten: een empirische vergelijking

Het hoofddoel van dit proefschrift was een empirische vergelijking tussen cyber-delinquenten en traditionele delinquenten op vier domeinen in de criminologie: daderschap gedurende de levensloop, persoonlijke en situationele risicofactoren voor daderschap en slachtofferschap, overeenkomst in deviantie van sociale netwerkleden en motivaties voor het plegen van verschillende clusters van delicten. Het onderzoek richt zich op nieuwe typen criminaliteit waarbij IT zowel het doelwit is als het belangrijkste middel is om het delict te plegen, de zogenoemde cyber-afhankelijke delicten (cybercrime in enge zin), zoals kwaadaardige hacking, defacing van websites, illegale controle over IT-systemen, gebruik van malware, et cetera. Deze delicten zijn een unieke test voor criminologische verklaringen voor daderschap, omdat deze delicten nog niet bestonden voor de opkomst van IT-systemen. De anonieme digitale context waarin deze delicten plaatsvinden, kan zorgen voor verschillen in bijvoorbeeld: situaties die gelegenheid bieden voor het plegen van criminaliteit, vaardigheden en persoonlijkheidskenmerken die nodig zijn om deze delicten te plegen, percepties van de consequenties van daderschap en verschillen in de dynamiek tussen daders en slachtoffers.

Resultaten

Daderschap gedurende de levensloop

In hoofdstuk 2 is gebruik gemaakt van een longitudinale dataset van registerdata voor de periode 2000-2012, voor het bestuderen van cyber-daderschap en traditioneel daderschap gedurende de levensloop. De resultaten lijken er op te wijzen dat sociale controle van anderen de kans op cyber-daderschap kan verlagen. Echter, sommige levensomstandigheden die voor traditionele criminaliteit een beschermende factor zijn, blijken gelegenheid te bieden voor cyber-delinquentie en blijkbaar is er onvoldoende controle van anderen in deze situaties om dit te voorkomen.

Voor persoonlijke levensomstandigheden is gevonden dat, in vergelijking met alleen wonen, samenleven met een partner of met een partner en kind de kans op cyber-daderschap verlaagt en alleenstaand ouderschap de kans op cyber-delinquentie verhoogt. Deze effecten waren in dezelfde richting en zelfs sterker voor cybercrime in vergelijking met traditionele criminaliteit. Wat betreft professionele levensomstandigheden is er geen statistisch significant effect gevonden van het hebben van werk of het volgen van een opleiding op cyber-delinquentie, terwijl dit wel een statistisch significant verlagend effect heeft op traditionele delinquentie. In de volledige daderpopulatie in dit onderzoek bleek dat werk in het algemeen de kans op cyber-delinquentie verlaagt, maar dat werk in de IT-sector en het volgen van een opleiding de kans op cyber-delinquentie verhoogt (niet statistisch significant).

Risicofactoren voor daderschap, slachtofferschap en slachtoffer-daderschap

Aan de hand van de cross-sectionele dataset die voor dit proefschrift is verzameld vergelijkt hoofdstuk 3 patronen in persoonlijke en situationele risicofactoren voor aparte groepen alleen-daders, alleen-slachtoffers en slachtoffer-daders, van cybercrime en traditionele criminaliteit. De resultaten laten een overlap zien tussen daderschap en slachtofferschap voor cybercrime. Voor zowel cybercrime als traditionele criminaliteit bleken slachtoffer-daders de meeste risicofactoren te hebben. Verschillen tussen de twee typen criminaliteit zijn voornamelijk te vinden in situationele risicofactoren die het resultaat lijken te zijn van de andere context waarin deze delicten plaatsvinden. Online activiteiten zijn belangrijker voor cybercrime, terwijl offline activiteiten belangrijker zijn voor traditionele criminaliteit.

Voor cybercrime bleken alleen-daders de relatief meer technische delicten te plegen in vergelijking met slachtoffers-daders. Dit was ook terug te zien in de risicofactoren voor alleen-daderschap, aangezien de kans op alleen-daderschap groter was indien een persoon meer IT-vaardigheden had, geen statistisch significant lage zelfcontrole had en online activiteiten had waarin criminele IT-vaardigheden konden toenemen. Voor slachtoffer-daders daarentegen waren IT-vaardigheden ook een risicofactor, maar minder dan voor alleen-daders. Daarnaast verhoogde een lage zelfcontrole de kans op slachtoffer-daderschap en meer algemene online routine activiteiten, waarin gelegenheden voor daderschap en risico's voor slachtofferschap zich kunnen voordoen, waren gerelateerd aan slachtoffer-daderschap.

Overeenkomst in deviantie van sociale netwerkleden

Aan de hand van de surveydata over het persoonlijke sociale netwerk van de respondenten is in hoofdstuk 4 de overeenkomst in deviantie van een persoon en dat van diens sociale netwerkleden vergeleken tussen cybercrime en traditionele criminaliteit. Er is een statistisch significante overeenkomst in deviantie gevonden voor cybercrime, maar de vergelijking met traditionele criminaliteit liet zien dat die overeenkomst veel zwakker was voor cybercrime.

Vervolgens bleek dat de overeenkomst in deviantie van sociale netwerkleden voor zowel cybercrime als traditionele criminaliteit sterker is voor netwerkleden van hetzelfde geslacht met wie de respondent dagelijks contact had. Echter, voor cybercrime bleek de overeenkomst het sterkst voor oudere sociale netwerkleden, terwijl het voor traditionele criminaliteit het sterkst is voor netwerkleden van dezelfde leeftijd. Dit wijst er op dat oudere rolmodellen belangrijker zijn voor cybercrime dan voor traditionele criminaliteit.

Clusters van delicten en gerelateerde motivaties

In hoofdstuk 5 is gebruik gemaakt van de zelfrapportage vragen uit de cross-sectionele dataset die voor dit proefschrift is verzameld. Hiermee is gekeken welke clusters van delicten er geïdentificeerd konden worden en in welke mate cyber-delinquenten te onderscheiden zijn van traditionele delinquenten. De analyses lieten zien dat cyber-afhankelijke criminaliteit zelden wordt gepleegd door daders die ook traditionele criminaliteit plegen. De clusters van cyber-delicten bestonden uit delicten die onderdeel zijn van dezelfde modus operandi, of delicten die gebruik maken van dezelfde vaardigheden en context.

Vervolgens zijn de zelf-gerapporteerde motivaties voor deze clusters van delicten in kaart gebracht en is geanalyseerd in hoeverre de clusters zich onderscheiden van de andere cluster aan de hand van de motivaties. De cyber-daders in deze sample rapporteerden bijna geen financiële motivaties. Intrinsieke motivaties, zoals nieuwsgierigheid en iets willen leren, waren het belangrijkst voor alle cybercrime clusters. Extrinsieke motivaties waren minder belangrijk voor cybercrime in vergelijking met traditionele criminaliteit. Echter, in de extrinsieke motivaties waren verschillen te zien tussen de cybercrime clusters. Hacking en internet-gerelateerde delicten werden vaker gepleegd om iets recht te zetten of een boodschap over te brengen en internet-gerelateerde delicten werden ook vaker gepleegd uit wraak, woede of om iemand te pesten. Indruk maken op anderen werd vrijwel nooit aangegeven als motivatie voor cyber-delinquentie.

Beperkingen

De samples die zijn gebruikt voor dit onderzoek zijn gebaseerd op politie en justitie data. Voor hoofdstuk 2 betekent dit dat het onbekend is in hoeverre een persoon ook daadwerkelijk schuldig was aan het plegen van het delict en in hoeverre deze persoon delicten heeft gepleegd in jaren waarin geen politiecontact is geweest. Voor hoofdstuk 3, 4 en 5 betekent dit dat de analyses laten zien welke risicofactoren, sociale contacten en motivaties in het heden zijn gerelateerd aan zelf-gerapporteerd daderschap in het heden, van personen die in het verleden (voorafgaand aan de zelfrapportage periode van 12 maanden) in contact zijn geweest met justitie voor het plegen van een delict. Vanwege het dark number in politie en justitie cijfers zijn dit selectieve samples. De resultaten gaan dan ook alleen over personen die in contact zijn geweest met politie of justitie voor het plegen van een delict.

Vanwege het karakter van de data in hoofdstuk 2 was er weinig diepgaande informatie over de verschillende variabelen. Registerdata bevat bijvoorbeeld geen informatie over de sterkte van iemands sociale relaties of daadwerkelijke dagelijkse activiteiten. De data die gebruikt is in hoofdstuk 3, 4 en 5 was meer diepgaand, maar het cross-sectionele karakter van deze data beperkte de mogelijkheid om sterke causale uitspraken te doen. Als laatste is de data gebaseerd op Nederlandse volwassenen. Het is niet bekend in hoeverre de resultaten ook van toepassing zijn op kinderen, jongeren of daders uit andere landen.

Toekomstig onderzoek

Replicatie van de onderzoekresultaten in andere en grotere samples, het liefst met longitudinale data, is noodzakelijk. Diepgaand longitudinaal onderzoek is nodig, bijvoorbeeld om: (1) de exacte causale processen en levensomstandigheden te vinden die het starten met of stoppen van cyber-delinquentie verklaren, (2) processen van selectie en beïnvloeding in online en offline sociale netwerken te identificeren en (3) de mogelijke causale relatie tussen daderschap en slachtofferschap te onderzoeken. Voor het gebruik van interventies die zijn gebaseerd op traditionele verklaringen voor delinquentie is het noodzakelijk om onderzoek te blijven doen naar de verschillen tussen cyber-delinquenten en traditionele delinquenten.

Toekomstig onderzoek kan zich richten op de vraag in hoeverre selectie en beïnvloedingsprocessen kunnen worden geïdentificeerd op bijvoorbeeld online fora en gaming communities. Dergelijk onderzoek kan indicaties geven voor de mate waarin online sociale contacten en online interacties vergelijkbaar zijn met traditionele sociale contacten en offline interacties. Daarnaast kan longitudinaal netwerk onderzoek waarin alle netwerkleden zelf rapporteren over hun cyber-deviantie inzicht bieden in (1) selectie en beïnvloedingsprocessen, (2) de discrepantie tussen verondersteld en daadwerkelijke cyber-deviantie van sociale contacten, (3) de verschillen tussen de invloed van daadwerkelijke en veronderstelde deviantie van sociale contacten op cyber-delinquentie en (4) de mate waarin de onzichtbaarheid van cyber-deviantie resulteert in een grotere discrepantie voor cybercrime in vergelijking met traditionele criminaliteit.

Kwalitatieve interviews kunnen meer gedetailleerde informatie verschaffen over bijvoorbeeld de rol van oudere rolmodellen of de strategie die delinquenten hebben als zij cyberdelicten plegen, bijvoorbeeld in hoeverre zij actief op zoek gaan naar gelegenheden voor het plegen van cybercrime dan wel zij deze gelegenheden toevalligerwijs tegenkomen tijdens hun dagelijkse activiteiten. Toekomstig onderzoek kan zich ook richten op de rol van IT-vaardigheden, bijvoorbeeld op verschillen in de mate waarin deze vaardigheden nodig zijn voor verschillende typen cyber-afhankelijke delinquentie, of in longitudinaal onderzoek op de manier waarop mensen IT-vaardigheden en kennis hoe ze deze kunnen misbruiken opdoen.

Praktische implicaties

Het is belangrijk om aan te geven dat geen van de preventie en interventie strategieeën die hier besproken worden empirisch geëvalueerd zijn voor cybercrime en dat deze aanbevelingen gebaseerd zijn op een klein aantal empirische onderzoeken. Daarom is het advies aan partijen die preventie en interventie programma ontwerpen om deze grondig te evalueren. Bij gebruik van interventies die gemaakt zijn voor traditionele delinquenten zal rekening moeten worden gehouden met empirisch vastgestelde verschillen tussen cyber-delinquenten en traditionele delinquenten. Het is niet aan te raden om de toepassing van traditionele interventies voor cybercrime enkel te baseren op niet-empirische aannames over verschillen of overeenkomsten.

Gebaseerd op de vergelijkingen in dit onderzoek is het te verwachten dat interventies erbij gebaat zijn om daders te stimuleren hun IT-gerelateerde nieuwsgierigheid op legitieme wijze te gebruiken. Een manier om dat te doen is om daders te helpen een legale baan te vinden waarin ze hun IT-vaardigheden kunnen gebruiken. Echter, is het erg belangrijk dat hierbij voldoende ethische begeleiding is en dat formele en informele sociale controle in het professionele leven wordt versterkt. Een andere veelbelovende methode om daders de juiste richting te geven is om ze een mentor toe te wijzen.

In interventies kan het belangrijk zijn dat daders van de meer technische cybercrimes wellicht rationeler handelen dan andere daders en dat ze dus beter in staat zijn om de verschillende manieren af te wegen waarop zij verantwoordelijk om kunnen gaan met beveiligingsproblemen. Daarnaast kunnen interventies er bij gebaat zijn om de perceptie van de gevolgen van cybercrime voor de dader en het slachtoffer te verhogen, bijvoorbeeld door zogenoemde ‘cease and desist visits’ of situationele criminaliteitspreventie.

Conclusie

De empirische vergelijking op de vier domeinen laat zien dat voorspellers voor cyber-delinquentie in zekere mate vergelijkbaar zijn met voorspellers voor traditionele delinquentie. Echter zijn er ook belangrijke verschillen in elk domein. Deze lijken het gevolg te zijn van de digitale context van cyber-delinquentie. Deze verschillen moeten in acht worden genomen wanneer traditionele verklaringen voor delinquentie worden gebruikt voor het verklaren van cyber-delinquentie. Voorspellers die gebaseerd zijn op traditionele verklaringen zullen moeten worden aangepast aan de digitale context en de sterkte van deze voorspellers zal empirisch moeten worden vergeleken tussen cybercrime en traditionele criminaliteit.

Dankwoord/Acknowledgements

Aan het proefschrift dat voor u ligt heb ik vier jaar lang hard maar vooral met veel plezier gewerkt. Met het risico dat ik mensen vergeet, wil ik op deze plaats graag een aantal mensen persoonlijk bedanken voor hun bijdrage aan de totstandkoming van dit proefschrift en/of hun bijdrage aan de geweldige aio-tijd die ik heb gehad.

Ten eerste mijn promotoren en copromotor. Ik heb ontzettend veel van jullie geleerd, juist omdat jullie het niet altijd met elkaar eens waren. Jullie hebben mij gestimuleerd om mijn eigen weg te gaan en mijn eigen keuzes te maken, terwijl jullie tegelijkertijd altijd bereid waren om met me mee te denken. Stijn, bedankt voor je eeuwige enthousiasme, nieuwsgierigheid en drive om mij van alles en nog wat te leren. Wim, bedankt voor de uitgebreide feedback die je altijd gaf op mijn werk en bedankt voor de rust en het overzicht die je altijd bracht. Jean-Louis, bedankt dat je me van begin af aan hebt gestimuleerd om meer uit mezelf te halen en nét dat stapje verder te gaan.

Dear Tom, thank you for giving me the opportunity to come to MSU and work with you on one of the chapters of this dissertation. I learned a lot from your perspective on my work. I am glad we already made plans for future collaborations.

I would like to thank the members of the manuscript committee and the promotion committee for their time and their attention to my work.

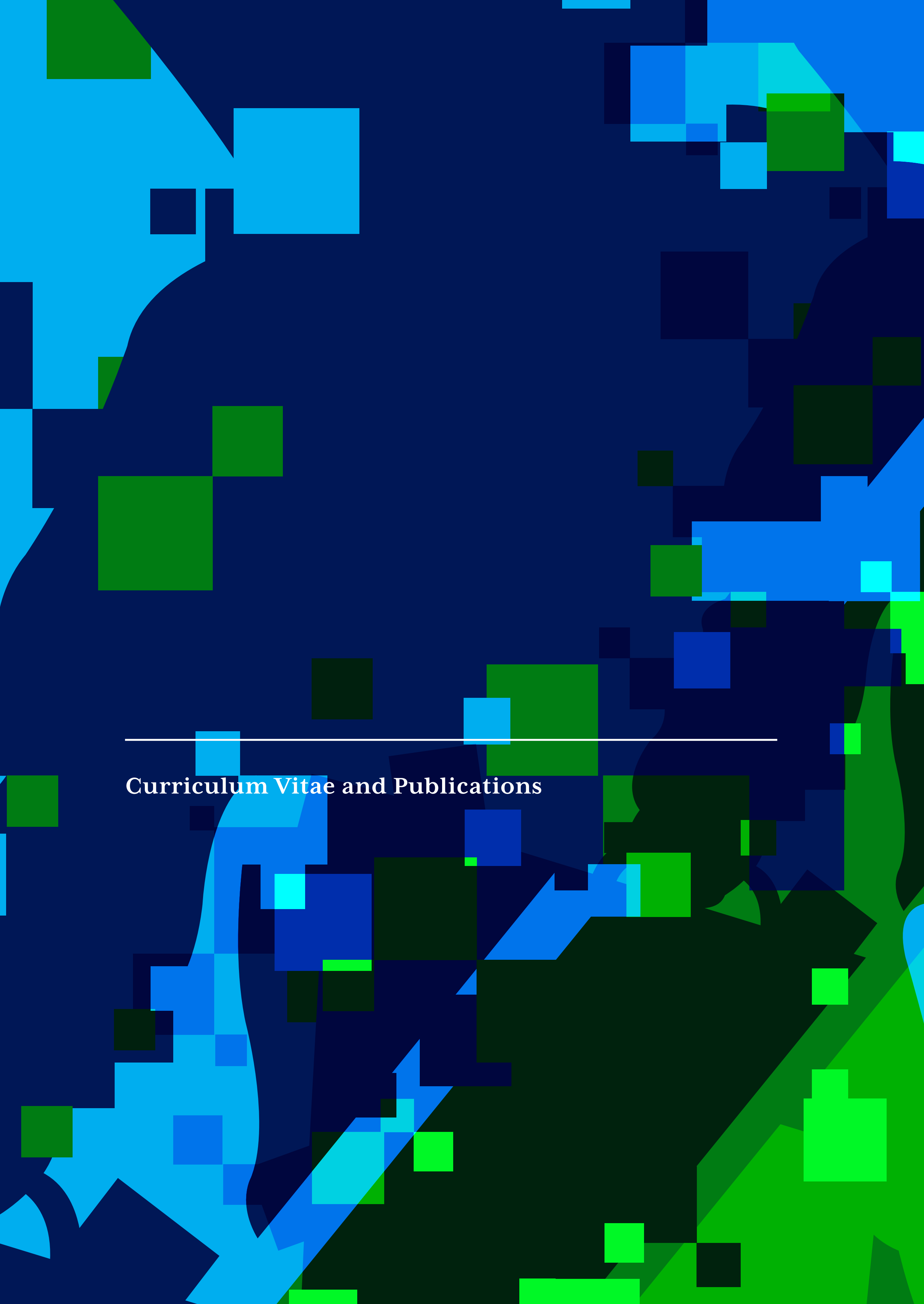
Ook de partners in het CyberCOP project zijn van onschatbare ware geweest voor dit onderzoek: het Team High Tech Crime van de politie, de High Tech Crime Unit van het Openbaar Ministerie en Reclassering Nederland. Specifiek wil ik graag Floor, Lisanne en Martine bedanken voor hun perspectief vanuit de praktijk. Daarnaast bedank ik graag alle deelnemers aan de bijeenkomst over de praktische implicaties van dit onderzoek voor hun input.

Tijdens de dataverzameling is Ho-Young erg behulpzaam geweest in de ontwikkeling en uitvoering van mijn survey, bedankt. Uiteraard wil ik ook de respondenten die de tijd hebben genomen om deel te nemen aan dit onderzoek hartelijk bedanken. Daarnaast was dit project niet mogelijk geweest zonder de Cyber Security research program subsidie van de Nederlandse Organisatie voor Wetenschappelijk Onderzoek.

Naast alle personen die inhoudelijk hebben bijgedragen aan mijn proefschrift wil ik graag mijn NSCR-collega's bedanken voor alle gezelligheid, grappen, lunchtafelgesprekken, borrels en eindeloze potjes tafeltennis. Jessica, Marre, Anne and Holly, I hope and believe that our friendship will continue even now that we are no longer colleagues. Jessica, I am glad you can also be my PhD-bridesmaid. I could not have wished for a better roommate and friend to share this experience with. Marre, Anne, and Holly, I have a lot of good memories from our time together, especially from our little road-trip.

Pap en mam jullie hebben mijn samen opgevoed tot wie ik nu ben en me alle kansen gegeven die ik nodig had om dit te kunnen bereiken. Mam, bedankt voor de liefdevolle interesse die je altijd toont in wat ik doe. Pap, wat had ik dit graag met je willen delen. Ik weet zeker dat je ontzettend trots op me zou zijn geweest. Karin, lieve zus, wat leuk dat ik straks samen met jou als mijn paranimf op het podium sta en we dit samen kunnen vieren.

Lieve Daniel, hoe leuk ik mijn werk ook vind, niets is zo belangrijk als het geluk en de liefde die wij samen hebben. Jij weet mij te stimuleren om mijn ambities waar te maken en jouw steun en luisterend oor zijn voor mij heel belangrijk, maar minstens zo belangrijk zijn de momenten dat we juist met hele andere dingen bezig zijn en we samen zoveel mogelijk van het leven genieten.



Curriculum Vitae and Publications

Curriculum Vitae

Marleen Weulen Kranenbarg (1990) obtained a BSc degree in Criminology from the Vrije Universiteit Amsterdam in 2012 and a MSc degree in Forensic Criminology from Leiden University in 2013. During her master she did an internship at the Netherlands Institute for the Study of Crime and Law Enforcement (NSCR) in Amsterdam. For that internship and her master's thesis she conducted a semi-experimental international comparative study on DNA-reports. Afterwards she continued working at the NSCR and started her PhD research on cyber-offenders that resulted in this dissertation. In September 2017 she started working as an Assistant Professor in Criminology at the Vrije Universiteit Amsterdam where she continues to do research on cybercrime and cybercriminals from a criminological perspective.

Publications

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*.

Weulen Kranenbarg, M., Van Der Laan, A., De Poot, C., Verhoeven, M., Van Der Wagen, W., Weijters, G. (2017). Individual Cybercrime Offenders. In E.R. Leukfeldt (Ed.), *Research Agenda: The Human Factor in Cybercrime and Cybersecurity.* Den Haag: Eleven International Publishing.

Leukfeldt, E.R., & **Weulen Kranenbarg, M.** (2017). De menselijke factor in cybercrime (Kroniek). *Tijdschrift voor Criminologie, 59*(3), 282-290.

De Keijser, J.W., Malsch, M., Luining, E.T., **Weulen Kranenbarg, M.**, & Lenssen, D.J.H.M. (2016). Differential reporting of mixed DNA profiles and its impact on jurists' evaluation of evidence. An international analysis. *Forensic Science International: Genetics, 23*, 71-82.

Malsch, M., De Keijser, J.W., Luining, E.T., **Weulen Kranenbarg, M.** & Lenssen, D.J.H.M. (2016). Hoe hard is DNA bewijs? Internationaal-vergelijkend onderzoek naar de interpretatie van DNA-profielen. *Nederlands Juristenblad, 18*, 1261-1266.

Van Gelder, J.L., Luciano, E.C., **Weulen Kranenbarg, M.**, & Hershfield, H.E. (2015). Friends with my future self: Longitudinal vividness intervention reduces delinquency. *Criminology, 53*(2), 158-179.