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\footnote{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.} 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.
1.3.1 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.

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%). 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.


References


147


References


