Cyber-offenders versus traditional offenders
An empirical comparison

Marleen Weulen Kranenbarg
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. 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 life 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) 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 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 (M years = 33.35, SD = 10.77) than those who committed traditional crimes (M years = 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). 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

---

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

<table>
<thead>
<tr>
<th>Variable</th>
<th>Prevalence rate (%)</th>
<th>Bivariate relationship (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Dutch population</td>
<td>Cyber-offender population</td>
</tr>
<tr>
<td>Household composition</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Alone</td>
<td>19.07</td>
<td>26.97</td>
</tr>
<tr>
<td>With partner</td>
<td>32.50</td>
<td>16.84</td>
</tr>
<tr>
<td>With partner &amp; child</td>
<td>32.24</td>
<td>26.71</td>
</tr>
<tr>
<td>With child</td>
<td>3.42</td>
<td>4.00</td>
</tr>
<tr>
<td>Other</td>
<td>12.76</td>
<td>25.48</td>
</tr>
<tr>
<td>Employment</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not employed</td>
<td>42.56</td>
<td>34.26</td>
</tr>
<tr>
<td>Employed non-IT</td>
<td>56.43</td>
<td>59.95</td>
</tr>
<tr>
<td>Employed IT</td>
<td>1.01</td>
<td>5.79</td>
</tr>
<tr>
<td>Education</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not in education</td>
<td>96.02</td>
<td>94.46</td>
</tr>
<tr>
<td>In non-IT education</td>
<td>3.85</td>
<td>4.44</td>
</tr>
<tr>
<td>In IT-education</td>
<td>0.13</td>
<td>1.10</td>
</tr>
<tr>
<td>Total (%)</td>
<td>100.00</td>
<td>100.00</td>
</tr>
<tr>
<td>N (person-years)</td>
<td>7,727,398</td>
<td>8,752</td>
</tr>
</tbody>
</table>

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 \(((1 - .69)\times100)\) 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

<table>
<thead>
<tr>
<th>Characteristic</th>
<th>Cybercrime</th>
<th>Traditional crime</th>
<th>Model comparison</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>OR  SE</td>
<td>OR  SE</td>
<td>χ²(df)</td>
</tr>
<tr>
<td>Household composition</td>
<td></td>
<td></td>
<td>11.66(4)*</td>
</tr>
<tr>
<td>Alone</td>
<td>- -</td>
<td>- -</td>
<td>-</td>
</tr>
<tr>
<td>With partner</td>
<td>.69* .11</td>
<td>.79*** .00</td>
<td>.75(1)</td>
</tr>
<tr>
<td>With partner &amp; child</td>
<td>.54*** .09</td>
<td>.81*** .00</td>
<td>5.79(1)*</td>
</tr>
<tr>
<td>With child</td>
<td>1.81* .53</td>
<td>1.07*** .01</td>
<td>2.83(1)†</td>
</tr>
<tr>
<td>Other</td>
<td>.84 .12</td>
<td>.98*** .00</td>
<td>1.04(1)</td>
</tr>
<tr>
<td>Employment</td>
<td></td>
<td></td>
<td>1.40(2)</td>
</tr>
<tr>
<td>Not employed</td>
<td>- -</td>
<td>- -</td>
<td>-</td>
</tr>
<tr>
<td>Employed non-IT</td>
<td>.90 .10</td>
<td>.93*** .00</td>
<td>.06(1)</td>
</tr>
<tr>
<td>Employed IT</td>
<td>1.14 .28</td>
<td>.89*** .01</td>
<td>1.02(1)</td>
</tr>
<tr>
<td>Education</td>
<td></td>
<td></td>
<td>.74(2)</td>
</tr>
<tr>
<td>Not in education</td>
<td>- -</td>
<td>- -</td>
<td>-</td>
</tr>
<tr>
<td>In non-IT education</td>
<td>1.10 .24</td>
<td>.92*** .01</td>
<td>.63(1)</td>
</tr>
<tr>
<td>In IT-education</td>
<td>1.06 .41</td>
<td>.88*** .03</td>
<td>.23(1)</td>
</tr>
<tr>
<td>Exposure days</td>
<td>1.12 .40</td>
<td>1.39*** .01</td>
<td>.38(1)</td>
</tr>
<tr>
<td>Days institutionalised</td>
<td>.52 .23</td>
<td>.69*** .01</td>
<td>.34(1)</td>
</tr>
</tbody>
</table>

N (person-years)     | 8,752      | 11,840,665        |
Unique personsa      | 870        | 1,144,740         |

All characteristics combined ($χ²(df)$) 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 ($χ²(df)$ = 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 ($\chi^2(df) = 5.79(1); p < .05$). 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 ($\chi^2(df) = 2.83(1); p<.10$).

**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 ($\chi^2(df) = 6.36(1); p<.05$; 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 ($\chi^2(df) = .01(1); p = .91$; 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 *Herkenningsdienstsystem*, 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; Sr161sexties; 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
References
References


References


References


References


