Article

European Journal of Criminology

European Journal of Criminology
1–21

DOI: 10.1177/1477370819849677
journals.sagepub.com/home/euc
SAGE

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

Marleen Weulen Kranenbarg
Vrije Universiteit (VU) Amsterdam, The Netherlands

Stijn Ruiter
Netherlands Institute for the Study of Crime and Law Enforcement, The Netherlands

Jean-Louis Van Gelder
University of Twente, The Netherlands

Abstract

The distinct setting in which cyber-dependent crime takes place may reduce the similarity in the deviance of social network members. We test this assumption by analysing the deviance of the most important social contacts of cyber-dependent offenders and traditional offenders in the Netherlands ($N = 344$ offenders; $N = 1131$ social contacts). As expected, similarity in deviance is weaker for cyber-dependent crime. Because this is a strong predictor of traditional offending, this has important implications for criminological research and practice. Additionally, for both crime types the offending behaviour of a person is more strongly linked to the deviance of social ties if those ties are of the same gender and age, and if the offender has daily contact with them. Implications and future criminological research suggestions are discussed.

Keywords

Cyber-dependent crime, cybercrime, ego-centred social networks, comparison traditional crime, social learning

Corresponding author:
Marleen Weulen Kranenbarg, Department of Criminology, Faculty of Law, Vrije Universiteit (VU) Amsterdam, De Boelelaan 1105, Amsterdam, 1081 HV, The Netherlands.
Email: m.weulenkranenbarg@vu.nl

Introduction

The expansion of the internet has created many new opportunities, including opportunities for cybercrime. Some traditional crimes, such as fraud, can now also be committed using IT systems. Such crimes are called ‘cyber-enabled’ or ‘cyber-assisted’ crime. New forms of crime, so-called ‘cyber-dependent’ crime, such as illegal hacking, defacing and taking control of IT systems, have also emerged (Levi et al., 2017; McGuire and Dowling, 2013; Wall, 2001). These crimes cannot be committed without using IT systems and therefore completely take place in an anonymous digital context where there are no physical social interactions (for example, Jaishankar, 2009; Suler, 2004; Yar, 2005, 2013) and offending requires IT skills and knowledge about how to use those skills illegally (Holt et al., 2010). These conditions challenge the extent to which criminological theories and established research findings also apply to these cyber-dependent crimes (for example, Jaishankar, 2009; Suler, 2004; Yar, 2005, 2013). Nevertheless, apart from some exceptions, most cybercrime research with a social learning perspective has focused on cyber-enabled or cyber-assisted deviant behaviour such as bullying, harassment, fraud, sexual deviance or piracy (for reviews, see Holt and Bossler, 2014; Jansen et al., 2017; Weulen Kranenbarg et al., 2017b) rather than on cyber-dependent offending.

Established empirical findings for traditional crime demonstrate a strong relationship between a person’s criminal behaviour and attitude, and the criminal behaviour and attitudes of that person’s social network (for example, Haynie and Kreager, 2013; Pratt et al., 2009; Warr, 2002; Weerman and Smeenk, 2005; Young and Rees, 2013). Research on cyber-dependent offending has shown that, compared with non-offenders, cyber-dependent offenders also more often have cyber-dependent deviant social contacts (for example, Holt et al., 2012a; Holt et al., 2010; Marcum et al., 2014; Morris, 2011; Morris and Blackburn, 2009; Rogers, 2001). Nevertheless, it is unclear if the digital context has an impact on the strength of this association. Is cyber-dependent crime different from traditional crime as regards the extent to which there is similarity in deviance among social network members? To date, this question has remained unanswered.

In order to examine this question, this article will empirically compare cyber-dependent offending with all other types of offending, which we refer to as ‘traditional offending’. These traditional offences include but are not limited to cyber-enabled and cyber-assisted offences. Because almost all traditional offences may include a digital component, cyber-enabled and cyber-assisted offences are less clearly distinguishable from traditional offline crime than cyber-dependent offences. Furthermore, cyber-dependent offences cannot be committed without using IT systems and, consequently, these heavily rely on the digital and anonymous context of these systems. Therefore, our arguments for less similarity in cyber-dependent deviance in social networks, provided later in this article, are most applicable to these cyber-dependent offences. Hence, these offences are our focus.

We use self-report data from an online survey among adult former crime suspects – traditional and cyber-dependent – in the Netherlands. In this survey, respondents reported not only on their own cyber-dependent deviant behaviour but also on the characteristics and behaviour of their most important social ties. We compare the relationship between cyber-dependent offending and cyber-dependent deviant network members with the relationship between traditional offending and traditional deviant network members. In addition, the structure of the data allows us to explore whether the relationship is stronger for contacts who are contacted daily and who are identical in age and gender.

Empirical similarity in behaviour of social ties for traditional and cyber-dependent crime

For traditional crime, numerous studies have found evidence for similarity in the deviant behaviour of social ties (for reviews, see Haynie and Kreager, 2013; Pratt et al., 2009; Warr, 2002; Young and Rees, 2013). Most studies focus on youth but, although the influence and time spent with friends decreases in adulthood (for example, Steinberg and Monahan, 2007), romantic partners may be of greater importance for adults. Further, adults have more freedom to select their own network members, which may result in more homogeneous networks (for example, Young and Rees, 2013). Longitudinal research on Dutch adults found support for the association in adult social networks (Rokven et al., 2017; Rokven et al., 2016). Additionally, it indicated that not all contacts show equivalent similarity in deviance, because similarity is stronger for more important social contacts, that is, those who are contacted daily.

For cyber-dependent crime, quantitative research has revealed that, in general, this type of offending is also more frequent if a person has friends who show cyber-dependent deviant behaviour or attitudes (Bossler and Burruss, 2011; Donner et al., 2014; Holt, 2007; Holt et al., 2012a; Holt et al., 2010; Holt and Kilger, 2008; Hu et al., 2013; Marcum et al., 2014; Morris, 2011; Morris and Blackburn, 2009; Rogers, 2001). In addition, qualitative studies disclosed that cyber-dependent offenders exchange IT knowledge, information on criminal opportunities, and neutralization techniques with online and offline friends and on forums (for example, Holt, 2007, 2009; Holt et al., 2012b; Hutchings, 2014; Hutchings and Clayton, 2016).

Underlying mechanisms of similarity in deviance

Despite the goal of this article being to test the strength of the above-mentioned similarity in cyber-dependent deviance of social ties, understanding the underlying theoretical mechanisms of this association is also important. Most cybercrime-related research uses a social learning perspective in explaining this association. From this perspective, differential association with delinquent peers will increase a person's likelihood of offending by imitation, adopting deviant definitions or attitudes, and differential reinforcement. Similarly, association with non-deviant social contacts can do the opposite and reduce offending, since these contacts disapprove of criminal behaviour (for example, Akers, 1998; Hirschi, 1969; Pratt et al., 2009; Sampson and Laub, 1993; Sutherland, 1947).

However, as discussed by Felson (1994, 1998), it is not only others' bad influence that could explain the association between the deviant behaviour of peers. Committing crimes in a group may be easier and more exciting than committing crimes on one's own, and when crimes are committed together it is the responsibility of the group instead of the individual. Individuals may therefore commit crimes in groups that they would not commit alone. In addition, this may stimulate an individual to select new social ties showing similar deviant behaviour (for example, Hirschi, 1969; Kalmijn, 1998; McPherson et al., 2001) because these ties can be a source of information, resources and accomplices. Moreover, deviant ties will be less likely to disapprove of criminal behaviour, which reduces the risk of negative social reactions and contacts reporting crimes to the police. In addition, social networks become even more homogeneous as daily activities generally increase the association with others who show similar behaviour. Moreover, existing deviant contacts may introduce new deviant social contacts, whereas non-deviant social contacts may end their relationship with an individual who commits crime (for example, Hirschi, 1969; Kalmijn, 1998; McPherson et al., 2001; Rokven et al., 2016).

Limitations of previous research on cyber-dependent crime

The existing evidence for similarity in cyber-dependent offending in social networks should be interpreted with some caution since several studies include traditional cyber-enabled or cyber-assisted deviance or more socially accepted deviance, such as online piracy. One reason that such studies focus on crimes requiring fewer IT-skills and IT-use could be explained by the fact that they use juvenile or college samples in which cyber-dependent offending is less common.

Another limitation of quantitative research is that it frequently focuses on the deviant behaviour of same-aged peers, whereas qualitative research has shown that older social contacts with more authority can act as mentors in learning to use IT skills for illegal purposes (Chiesa et al., 2008; Holt et al., 2010). In addition, previous research generally measured the deviance of all peers in one item that reflects the overall deviance in the peer network. Therefore, possible differences between social contacts, related to contact frequency or similarity in characteristics, have not yet been studied. In addition, these studies have not been able to control for similarity in other characteristics that could have influenced the similarity in the 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 relationship between their behaviour may be partly spurious, therefore.

Most importantly, however, previous research failed to empirically compare the strength of similarity in deviance in social networks between cyber-dependent crime and traditional crime. Studies have focused on applying social learning to cyber-dependent crime, claiming that, for example, imitation may be more important for learning skills when compared with traditional crime, thereby missing arguments that could imply that there is less similarity in the deviant behaviour of strong social ties for cyber-dependent crime.

In short, previous research showing an association between the cyber-dependent deviant behaviour of social ties has three important limitations. First, juvenile or college samples limited most studies to cyber-enabled offending instead of cyber-dependent offending. Second, the general measurement of overall peer delinquency limited the evidence for the association to same-aged peers, for which it was not possible to compare between peers or control for similarity in age or gender. Lastly, it is unknown to what extent the association is just as strong for cyber-dependent offending as it is for traditional offending, because there are no empirical comparisons of similarity in deviance between these two categories. This article is a first step in addressing these issues. In addition, the future research suggestions in the discussion section may further develop this field.

Less similarity in cyber-dependent deviance in strong social networks

Both the anonymous context in which cyber-dependent crimes take place and the wealth of information on the Internet regarding how to commit these crimes may reduce the importance of having strong social ties who are also committing cyber-dependent crimes. As Goldsmith and Brewer (2015) discuss, learning the skills for cyber-dependent criminal behaviour can be done in a self-directed way, by browsing the Internet for information. In line with that argument, qualitative studies show that, although some hackers also have offline social contacts who hack, they mainly operate alone and learn their skills from Internet sources such as forums and by trial and error (Holt, 2007, 2009). Even though it could be argued that these forums are also a source of social learning or offender convergence settings that could facilitate co-offending (Soudijn and Zegers, 2012), the social contacts on these forums are not likely to be the type of social ties that traditionally show the strongest association in offending, that is, strong, usually face-to-face social ties (for example, Agnew, 1991; Rokven et al., 2017).

In addition, non-deviant social contacts may also have less influence on cyber-dependent offending. Several authors (for example, Jaishankar, 2009; Suler, 2004; Yar, 2013) have theorized that the digital context changes behaviour because of anonymity and a lack of connection with the 'real' world. They argue that behaviour in this context is less visible and people often feel the online world is disconnected from the offline world. Consequently, they think their online behaviour does not have any offline consequences. In addition, apprehension rates for cybercrimes are very low (for example, Leukfeldt et al., 2013) 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 owing to negative social consequences (for example, Jaishankar, 2009; Suler, 2004; Yar, 2013). This could decrease the perception that these crimes will have any negative consequences on an individual's social life. We argue that this lack of visibility and the perception that cyber-dependent offending will not affect social relationships may decrease the influence of social contacts.

For the same reason, a cyber-dependent offender may not have to consider the attitudes of new social network members towards cyber-dependent offending when selecting those network members. In addition, the invisibility of cyber-dependent offending 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 (for example, Holt, 2009; Holt et al., 2010; Holt and Kilger, 2008). In sum, we argue that the digital context in which cyber-dependent crimes take place may result in a smaller association between the cyber-dependent deviant behaviour of social ties compared with traditional deviant behaviour.

The current study

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

> Is the relationship between an individual's cyber-dependent deviant behaviour and the cyber-dependent deviance of strong social ties different from the relationship between traditional deviant behaviour and the traditional deviance of strong social ties?

Based on previous cybercrime research we expect to find a relationship between an individual's cyber-dependent deviant behaviour and the cyber-dependent deviance of social network members (Hypothesis 1) but, based on the arguments above, we expect that this relationship is weaker for cyber-dependent crime (Hypothesis 2) compared with traditional crime. Additionally, our data include separate observations for the most important social contacts in a person's life, which enables us to control for similarity in gender and age between a person and a social network member. In addition, this enables us to explore whether or not cyber-dependent crime is comparable to traditional crime concerning the manner in which the relationship between an individual's behaviour and the behaviour of social contacts differs between contacts. Hence, we also explore:

> Are there differences in the relationship between an individual's cyber-dependent deviant behaviour and the cyber-dependent deviance of social ties for different network members (daily/non-daily contacts, same gender/other gender, same age/older/younger) and are these patterns comparable to those for traditional deviance?

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

Data and methods

Sample and procedure

For this study, we selected all 1100 cyber-dependent crime suspects and a random sample of 1127 traditional crime suspects from the prosecutor's office database in the Netherlands for the period 2000–2013. Being registered as a suspect in this database means that the police have sufficient reason to suspect a person and therefore send the case to the public prosecutor. It is known that about 90 percent of these suspects will be convicted or settle out-of-court with the public prosecutor (Blom et al., 2005). Of this sample, 928 cyber-dependent crime and 875 traditional crime 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 also included the option to complete the survey on paper (used by three respondents from the traditional crime sample) or through a Tor Hidden Service website (used by three respondents from the cyber-dependent crime sample).[1] The invitation letter also mentioned scope, confidentiality and anonymity, and the €50 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, scope and content of the survey.

The response rate of traditional crime suspects was lower than that of cyber-dependent crime suspects. Because we aimed for two equal-sized samples, we sent reminder letters after two and four weeks to the traditional suspects. After six weeks, 268 cyber-dependent crime suspects (28.88 percent) and 141 traditional crime suspects (16.11 percent) 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 percent) participated and the final sample comprised 268 cyber-dependent crime suspects and 267 traditional crime suspects, response rates of respectively 28.88 percent and 16.12 percent.

Measures

Alters. By using a name-generator/interpreter method (McCallister and Fischer, 1978), our respondents – who will be referred to as ‘egos’ in the remainder of the article – were asked to name up to five important personal social network members – ‘alters’ in the remainder of the article – with whom they had discussed important things in the preceding 12 months. This type of network is called a core discussion network. Because these are a person’s most important social ties, their behaviour is generally most similar to that of the respondent. The deviance of these social ties in core discussion networks has also been found to be very important in predicting traditional criminal behaviour (Rokven et al., 2017; Rokven et al., 2016). Participants were given the opportunity to use non-identifying aliases rather than the real names of their network members. These names were then used to ask respondents about the alter’s cyber-dependent and traditional deviance, contact frequency, the alter’s age and gender, and their relationship with the alter. Among all egos included in the analysis, the average number of alters was 3.3 (SD = 1.4, Median = 3; 47.7 percent friends, 35.5 percent family members, and 16.8 percent partners), 55.2 percent of the alters were male and they were on average 40.3 years old.

Dependent variables. Alters’ cyber-dependent deviance was measured by combining two questions: ‘As far as you know, did this person commit online (digital) criminal offences in the past 12 months?’ (yes–no) and ‘In general, what does this person think about committing online (digital) criminal offences?’ (‘Mostly approves of it’, ‘Sometimes approves

Table 1. Descriptive statistics.

Egos		Alters	
Dichotomous variables	Percent	Dichotomous variables	Percent
Cyber-dependent offender	19.11	Cyber-dependent deviant alter	7.60
Traditional offender	22.33	Traditional deviant alter	4.24
Male	78.49	Daily contact alter	44.15
Continuous variables	Mean	Alter same gender as ego	60.53
Low self-control	1.75	Alter same age as ego	9.20
IT-skills	4.53	Alter younger than ego	43.41
Age[a]	36.80	Alter older than ego	47.39
Level financial problems	0.23		
N	344	*N*	1131

Note:
a. In the analyses, age started at 0 (age minus 17) and models included age, age-squared and age-cubed.

sometimes disapproves of it', or 'Always disapproves of it'). Two similar questions on offline (non-digital) criminal offences were used for measuring alters' traditional deviance. For both types of deviance, examples were provided that reflected the crimes in the ego self-report questions (see below). Alters were considered cyber-dependent or traditional deviants if they had committed a cyber-dependent crime or traditional crime or mostly approved of committing a cyber-dependent crime or traditional crime, so both types were measured as dichotomous dependent variables (1 = deviant alter; see Table 1 for descriptive statistics of dependent and independent variables). This means that we analyse two dependent variables for each reported alter, cyber-dependent deviant alter and traditional deviant alter.

Independent variables. Offending conducted by the respondent was included as a dichotomous variable (1 = offender) that indicated whether or not a respondent self-reported having committed at least one cyber-dependent crime or traditional crime in the preceding 12 months. Based on the Dutch National Cyber Security Centre (2012) list of cyber-dependent crimes and the Computer Crime Index of Rogers (2001), 13 different cyber-dependent crimes were included. These were: hacking by guessing passwords (7.9 percent), data theft (6.5 percent), defacing (6.2 percent), other types of hacking (5.3 percent), damaging data (4.4 percent), phishing (3.8 percent), taking control over an IT system (3.5 percent), intercepting a communication (2.6 percent), malware use (2.4 percent), DoS attacks (2.4 percent), selling somebody else's data (1.5 percent), spamming (1.5 percent), and selling somebody else's credentials (0.9 percent). Based on Svensson et al. (2013) and Dutch criminal law, 11 traditional offences were included. These were: tax fraud (7.7 percent), stealing (6.4 percent), threats (5.0 percent), buying or selling stolen goods (5.6 percent), carrying a weapon (5.0 percent), violence (5.3 percent), vandalism (4.4 percent), selling drugs (3.8 percent), insurance fraud (3.5 percent), burglary (1.5 percent), and using a weapon (1.2 percent).

As discussed in the introduction, the most important step in examining the relationship between an individual's cyber-dependent deviant behaviour and the cyber-dependent deviance of their strong social network members is to test the strength of this association in comparison with that found for traditional deviance. Because this association has generally been found to be strong for a very diverse group conducting traditional crime, this study will compare the general association for traditional crime with the association for cyber-dependent crime. Therefore, cyber-dependent offending and traditional offending were measured as dichotomous variables in this study.

The similarity of alters and ego was constructed by comparing the reported gender and age of alters with those of ego. Alters were classified as younger, exactly the same age or older, and as same or different gender. The dichotomous variables on similarity in age and gender were included in additional analyses to test whether or not the estimated association in deviance changed. For the second research question, it was also measured whether or not ego had daily contact with an 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 made online or offline phone calls. If one of these questions was answered with 'daily', alters were considered to be daily contacts. For the second research question, the different alter classifications were used to include the dichotomous main effects of the offending of ego for different deviant alters. For example, if the dichotomous variable 'offender–same age' equals 1 for cyber-dependent crime, ego is a cyber-dependent offender and exactly the same age as alter.

In addition to ego's offending, we included ego's low self-control and IT skills. It is important to control for low self-control because it could potentially influence both the likelihood of offending and the likelihood of selecting deviant friends or being influenced by deviant friends, as argued by Gottfredson and Hirschi (1990). Furthermore, analogous to traditional crime, studies have shown that low self-control is a predictor of cyber-dependent offending, even when social learning measures are included (for example, Bossler and Burruss, 2011; Donner et al., 2014; Holt et al., 2012a; Hu et al., 2013; Marcum et al., 2014; Weulen Kranenbarg et al., 2017a). Therefore, it is important to measure to what extent low self-control is related to having cyber-dependent deviant social ties. Low self-control was constructed with items from the HEXACO-SPI-96 personality inventory (De Vries and 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).[2] The scale was reverse coded to a low self-control scale.

Previous research has found a link between IT skills and cyber-dependent offending (Holt et al., 2012a; Morris and Blackburn, 2009; Weulen Kranenbarg et al., 2017a) and some research has claimed that the IT skills necessary to commit cyber-dependent crimes could be learned from deviant friends by imitation (for example, Holt et al., 2012a; Holt et al., 2010; Morris and Blackburn, 2009). Therefore, we included ego's IT skills in our analyses as well, to see to what extent having a cyber-dependent deviant alter is related to IT skills. IT skills were measured with an IT skills test consisting of 10 knowledge questions ranging from very easy (such as '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 92.5 percent of the respondents), to very challenging questions, such as a piece of code that contained a bug and respondents had to indicate which techniques could be used to prevent misuse of this bug (answered correctly by only 4.3 percent; see Supplemental material for all the questions). The IT skills measure used in this study reflects the number of correct 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 et al. (2012a).

Other control variables were gender (1 = male), age (age−17, and age-squared and age-cubed), and the level of financial problems in the preceding 12 months (an adjusted version from The Prison Project; Dirkzwager and Nieuwbeerta, 2015). Respondents indicated whether or not the following situations had occurred (1 = yes): 1. 'saved money' (reverse coded); 2. 'had just enough money to live on'; 3. 'had problems with making ends meet'; 4. 'not been able to replace broken stuff'; 5. 'had to borrow money for essential expenses'; 6. 'pawned belongings'; 7. 'had creditors/bailiffs at my door'; 8. 'had debts of 5000 euros or more'. The sum of all items was divided by eight to obtain a scale from 0 to 1 (Cronbach's $\alpha = 0.83$). In addition, we controlled for initial differences between cyber-dependent crime and traditional suspects with a dichotomous initial group variable (1 = cyber-dependent sample). This ensures 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-dependent deviant contacts or IT skills.

Non-response

For the sample of traditional suspects, females were overrepresented among respondents (20.8 percent females among respondents compared with 13.8 percent in the original sample, $\chi^2(1) = 5.93, p < .05$). No other statistically significant differences in gender or age were found between respondents and non-respondents in the non-response analyses. For both cyber-dependent crime and traditional crime, respondents who named at least one social network member were slightly more delinquent compared with respondents who did not name a social network member, but these differences were not statistically significant (cyber-dependent crime: 15.1 versus 18.8 percent; traditional crime: 15.1 vs. 22.0 percent). In total, 364 respondents reported 1220 social network members. From these alters, 89 (7.3 percent) were excluded because of missing values on one of the dependent variables, resulting in a final sample of 1131 alters and 344 egos.

We used the Stata 14 Multivariate Imputation by Chained Equations (MICE) procedure (based on Royston, 2004) for multiple imputation of missing values for the independent variables of 268 observations (ego–alter combinations, 23.1 percent). In line with Von Hippel (2007), cases with missing values on the dependent variables were used in the imputation procedure but excluded from the analyses in this article. We imputed 20 datasets, which were used for estimating the models, while adjusting the coefficients and standard errors for the variability between imputations according to Rubin (1987) combination rules.

Analytical strategy: Multilevel logit models

For analysing our two binary outcome variables, we used logit models. Our data have a hierarchical structure in which the two outcome variables at the alter level are nested in

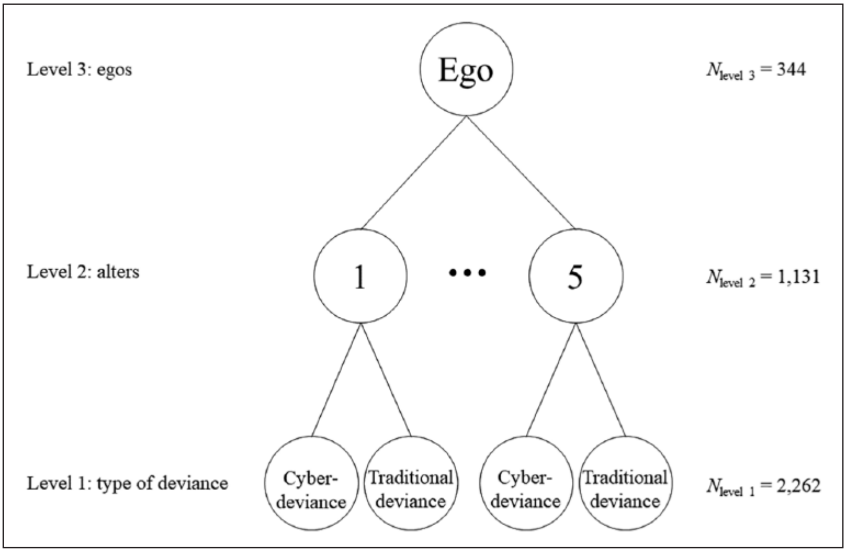
Level 3: egos
Ego
$N_{\text{level 3}} = 344$
Level 2: alters
1
•••
5
$N_{\text{level 2}} = 1{,}131$
Level 1: type of deviance
Cyber-deviance
Traditional deviance
Cyber-deviance
Traditional deviance
$N_{\text{level 1}} = 2{,}262$

Figure 1. Schematic overview of multilevel structure.

alters and, because egos could name multiple alters, these are further nested in egos. This nested structure violates the independence of observations assumption of standard logit regression. For this reason and in line with Rokven et al. (2016), we account for the autocorrelation among our observations by estimating multilevel logistic models in which the two deviance measures (level 1) were nested in alters (level 2), which were nested in egos (level 3). See Figure 1 for a schematic overview of the nesting structure. We used the Stata 14 meqrlogit command to estimate three-level logistic regression models with random intercepts at levels 2 and 3. Because the two dependent deviance measures were analysed simultaneously, we included a dummy variable for the type of deviance (cyber-dependent deviance item = 1) and the independent variables were included in the model separately for the two types of deviance by multiplying the independent variables by the item type. To test for effect differences between cyber-dependent and traditional offending, we used Wald Chi-squared post-estimation tests for multiply imputed data (see StataCorp, 2017).

Results

The parameter estimates of the multilevel logistic regression model in Table 2 are presented as odds ratios, which reflect how many times the odds an alter was deviant are multiplied with a one-unit increase in the independent variable, for example if ego is an offender. The final column shows the Wald Chi-squared post-estimation test for the statistical comparison between the estimates for cyber-dependent crime and for traditional crime. Our most important finding is that the relationship between egos' cyber-dependent offending and their alters' cyber-dependent deviance is statistically significantly weaker for cyber-dependent offending than for traditional offending ($F(1) = 3.64$, $p < .10$).

Table 2. Multilevel logistic regression for deviance of alter ($N_{\text{level 1}} = 2262$, $N_{\text{level 2}} = 1131$, $N_{\text{level 3}} = 344$).

	OR	95% CI		Comparison[d]
		LL	UL	*F*(df)
Ego offender[a]				3.64(1)†
Cyber-dependent crime	4.53*	1.37	14.94	
Traditional crime	24.06***	5.03	115.09	
IT skills				1.17(1)
Cyber-dependent crime	1.20	0.87	1.65	
Traditional crime	1.00	0.67	1.48	
Low self-control				1.74(1)
Cyber-dependent crime	2.01	0.45	9.03	
Traditional crime	5.60†	0.84	37.08	
Financial problems				5.88(1)*
Cyber-dependent crime	2.00	0.20	19.82	
Traditional crime	0.06†	0.00	1.47	
Male				3.02(1)†
Cyber-dependent crime	6.30*	1.08	36.73	
Traditional crime	1.49	0.21	10.61	
Age				1.77(1)
Age				
Cyber-dependent crime	0.92	0.80	1.06	
Traditional crime	0.90	0.69	1.19	
Age-squared				
Cyber-dependent crime	1.00	0.99	1.00	
Traditional crime	0.96	0.91	1.01	
Age-cubed				
Cyber-dependent crime	1.00	1.00	1.00	
Traditional crime	1.00†	1.00	1.00	
Cyber group[b]				1.43(1)
Cyber-dependent crime	1.13	0.28	4.51	
Traditional crime	2.72	0.49	15.13	
Cyber-dependent deviance item[c]	7.42**	1.94	28.40	
Constant	0.00***	0.00	0.01	

Notes: All variables were centred on the mean.

a. For cyber-dependent crime this reflects the estimate for a cyber-dependent offending ego; for traditional crime this reflects the estimate for a traditional offending ego.

b. 1 = originates from cyber-sample.

c. Dummy variable for the type of deviance (1 = cyber-dependent deviance item). The positive effect of this variable indicates, in line with Table 1, that more alters are cyber-dependent deviant than traditional deviant.

d. Wald Chi-squared post-estimation test.

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

Although we find a statistically significant positive relationship for cyber-dependent crime, in line with Hypothesis 1, this relationship is much weaker compared with traditional crime, in line with Hypothesis 2. Whereas ego's traditional offending increases the odds that alters are traditionally deviant 24.06 times, the odds that alters are cyber-dependent deviants are increased only 4.53 times when a respondent is a cyber-dependent offender compared with when s/he is not. Additional analyses showed that these estimates hardly changed when age and gender similarity were accounted for.[3]

In addition, we found that alters are more likely to be cyber-dependent deviants if ego is a male. We found no statistically significant effects for IT skills, financial problems or lower self-control of ego on the odds that alters are cyber-dependent deviants. In contrast, the effect of low self-control is marginally statistically significantly related to the odds that alters are traditional deviants, but the effect size difference turned out to be not statistically significant. A joint Wald Chi-squared post-estimation test of all effect size differences showed that the estimates for cyber-dependent crime and traditional crime are statistically significantly different ($F(9) = 2.74, p < .01$).

Results pertaining to our second research question can be found in Table 3. For both cyber-dependent crime as well as traditional crime, the similarity in deviant behaviour is stronger for alters who are contacted daily and who are of the same gender and age as ego. This corroborates Hypotheses 3 and 4. Overall, and in line with Hypothesis 2, the estimates in these models are also stronger for traditional crime. The final column, with the statistical test of effect size differences, indicates that for each model at least one estimate is marginally stronger. There are two differences in these patterns. Cyber-dependent offending of ego is statistically significantly related to cyber-dependent deviance of alters only if ego and alter are of the same gender. For traditional crime, we see that offending of ego is also statistically significantly related to the deviance of alter if they have a different gender. In addition, for both traditional crime and cyber-dependent crime, the relationship in deviance is strongest for egos and alters of the same age. However, for cyber-dependent crime, the second strongest relationship is found when alters are younger than ego, whereas for traditional crime that is when alters are older.

It should be noted, however, that there were no statistically significant effect size differences for different social contacts, either for cyber-dependent or for traditional crime.[3] As an example, although the odds ratio for a same-gender cyber-dependent offender is 6.60 and the odds ratio for another-gender cyber-dependent offender is only 2.04, the Wald Chi-squared post-estimation test showed that these effects were not statistically significantly different ($F(1) = 2.11, p = .15$). This means that we find no support for Hypotheses 3 and 4, although the effects are in the expected direction.

Conclusion

In this article 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 (for example, Jaishankar, 2009; Suler, 2004; Yar, 2013) 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 relationship between an individual's deviant behaviour and the deviance of social

Table 3. Multilevel logistic regression models for deviance of alter for different alters ($N_{\text{level 1}} = 2262$, $N_{\text{level 2}} = 1131$, $N_{\text{level 3}} = 344$).

	OR	95% CI		Comparison[b]
		LL	UL	F(df)
0. Ego offender[a]				3.64(1)†
Cyber-dependent crime	4.53*	1.37	14.94	
Traditional crime	24.06***	5.03	115.09	
1. Ego offender – alter daily contact				2.98(1)†
Cyber-dependent crime	4.89*	1.28	18.72	
Traditional crime	24.48***	4.74	126.42	
Ego offender – alter non-daily contact				2.80(1)†
Cyber-dependent crime	4.15†	1.00	17.30	
Traditional crime	23.75***	4.09	137.99	
2. Ego offender – alter same gender				3.07(1)†
Cyber-dependent crime	6.60**	1.85	23.55	
Traditional crime	32.10***	6.19	166.58	
Ego offender – alter other gender				2.62(1)
Cyber-dependent crime	2.04	0.38	10.96	
Traditional crime	13.60**	2.29	80.62	
3. Ego offender – alter same age				1.44(1)
Cyber-dependent crime	11.47*	1.66	79.40	
Traditional crime	46.11***	6.68	318.28	
Ego offender – alter younger				1.94(1)
Cyber-dependent crime	4.42*	1.04	18.85	
Traditional crime	20.18***	3.39	119.96	
Ego offender – alter older				3.52(1)†
Cyber-dependent crime	3.65†	0.90	14.71	
Traditional crime	22.85***	4.13	126.30	

Notes: All estimates reflect the effect of an offending ego compared with all non-offending egos. For example, for daily contact the estimate 'ego offender – alter daily contact' reflects the estimate of an offending ego who has daily contact with alter, compared with all non-offending egos, with both daily and non-daily contact with alter. Models included all variables from the original model. This table shows only variables of interest. Complete models can be requested from the first author. All variables were centred on the mean.

a. For cyber-dependent crime this reflects the estimate for a cyber-dependent offending ego, for traditional crime this reflects the estimate for a traditional offending ego.

b. Wald Chi-squared post-estimation test.

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

network members would be weaker for cyber-dependent crime compared with traditional crime. We tested this hypothesis by using data on the most important social ties from an online survey among a high-risk sample of cyber-dependent and traditional former crime suspects in the Netherlands. We contributed to the literature on cybercrime by specifically addressing less common cyber-dependent offending and comparing it to traditional offending in an understudied adult offender population. In contrast to previous research, we studied the most important social contacts, not only same-aged peers, and we compared differences in terms of contact frequency and similarity between social contacts.

In line with our expectations, our comparison showed that the relationship between the cyber-dependent deviance of important social network members and a person's cyber-dependent criminal behaviour is much weaker for cyber-dependent crime compared with traditional crime. Even when controlling for similarity in age and gender between a person and social network members, our study, just like previous studies, showed that there is a statistically significant relationship in the cyber-dependent deviance of social ties. More importantly, however, the finding that this relationship is much weaker for cyber-dependent crime puts this previous research into perspective.

Previously, this criminological research on cyber-dependent crime has focused on examining the relationship in deviant behaviour of social ties. Even though this proves to be valuable, because there is a relationship, our analyses show that it may not be as valuable as it is for traditional crime. Our results and the arguments we provided in the introduction could suggest that, compared with traditional offenders, cyber-dependent offenders may not need the traditional deviant strong social contacts to commit cyber-dependent crimes, because they may learn their offending skills from completely different sources. Moreover, because of the anonymous digital context in which these crimes take place, cyber-dependent offenders may also be more indifferent towards their strong social contacts' negative or positive social reactions when they commit crimes in this context (for example, Jaishankar, 2009; Suler, 2004; Yar, 2013). Therefore, the deviance of social contacts may have less influence on cyber-dependent deviant behaviour, and/or networks of strong social ties may not become more homogeneous because people may not consider the attitudes of their social contacts towards cyber-dependent deviant behaviour when becoming friends with them. In short, our results show the value of examining cyber-dependent crime in comparison with traditional crime when applying traditional criminological theories to cyber-dependent crime. In that way, differences in the strength of the correlates can indicate to what extent social network-based prevention strategies, designed for traditional crime, are expected to have a similar effect on cyber-dependent crime. This comparison makes the large body of criminological research on traditional crime also more useful in understanding cyber-dependent crime.

In addition to our main finding, males were more likely to have cyber-dependent deviant social ties. Interestingly, although IT skills are usually related to cyber-dependent offending, these are not related to having cyber-dependent deviant social ties. This may indicate that not all IT skills necessary for cyber-dependent offending are learned from strong social contacts, for example by imitation. In combination with the weaker similarity in deviant behaviour, this indicates that IT skills are also acquired in another way, for example by reading information online (for example, Goldsmith and Brewer, 2015; Holt, 2007, 2009; Holt et al., 2010; Holt and Kilger, 2008). Partly in line with what has been found for hacking by Holt et al. (2012a), this study disclosed no statistically significant relationship between low self-control and having a cyber-dependent deviant social tie.

Lastly, our data structure also 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 cyber-dependent crime and traditional crime. However, the results pointed in the direction of our expectation that the relationship is stronger for same-gender, same-age and daily-contacted social network members. Even though previous studies have shown that older mentors can be important in a social learning process for cyber-dependent crime (for example, Chiesa et al., 2008; Holt et al., 2010), the relationship between offending and having deviant social contacts is strongest for same-aged peers. Nevertheless, because there also is a relationship for younger and older social contacts, criminological research on cyber-dependent crime may benefit from analysing other social ties too.

Discussion

The present study had several limitations that merit discussion. Self-report data have their limitations and, owing to the cross-sectional nature of our data, it was not possible to study the underlying mechanisms of the association between the deviant behaviour of social ties. As discussed in the introduction with regard to the underlying mechanisms, there are several ways in which social ties may influence an individual's criminal behaviour, while at the same time there may be a selection process in which a person prefers to become friends with social ties who show similar behaviour. Therefore it is essential that future research in this area uses longitudinal designs, because that enables a distinction between the selection and influence processes of social ties, and this could, for example, shed light on how people acquire IT skills and knowledge on illegal use of those skills over time. Such a study could also include traditional offending, because that will further inform us about the way the digital context of cyber-dependent crime may have an impact on the underlying mechanisms of this association.

If future studies are able to shed light on the underlying mechanisms of selection and influence, these studies could further focus on the explanatory power of different social learning components (that is, differential association, deviant definitions, imitation, reinforcement; Akers, 1998). Some previous studies, for example, suggest that imitation is more important for cyber-dependent crime because it can be a way to learn IT skills (for example, Holt et al., 2010). However, this claim is not in line with our finding that IT skills are not related to having cyber-dependent deviant social contacts and the consistent finding that IT skills still predict cyber-dependent offending when the deviance of social contacts is included in the analyses (for example, Holt et al., 2012a; Holt et al., 2010; Morris and Blackburn, 2009).

Another limitation of this study is that it has been shown that, when asking people to indicate the deviance of their social ties, they may project their own behaviour onto their network members, which results in an overestimation of similarity (for example, Boman et al., 2016; Weerman and Smeenk, 2005; Young et al., 2014). Because respondents may not be aware of the deviance of their social network members, we specifically asked the respondents to report on their alters' deviance only as far as they knew about it. As a consequence, we could analyse the similarity in deviance among social network members only for behaviour and attitudes that our respondent knew about. Because the theoretical underlying mechanisms all assume that a person knows about the deviance of social contacts, our study still resulted in very relevant information on the extent to which this known deviance of social ties is related to the deviance of an individual. For cyber-dependent crime it may be even harder to know about the actual behaviour and attitudes of contacts because 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-dependent deviance compared with traditional deviance in our sample. In addition, in line with previous research (for example, Rokven et al., 2016), we see much higher levels of self-reported offending than perceived deviance of social contacts for both cyber-dependent crime and traditional crime.

Based on the limitations above, future studies would benefit from using a social network method similar to the one used in Weerman and Smeenk (2005), where the network members report on their deviant behaviour themselves. This would increase our knowledge concerning people's ability to know about their social contacts' cyber-dependent deviance and the differences between similarity in perceived and actual deviance in social networks for cyber-dependent crime. Co-offending, one of the other underlying reasons for selection and influence, could also be measured in these networks. This could also tell us to what extent people know about each other's cyber-dependent deviance, because they commit these crimes together.

It has been shown in the past that the deviance of peers differs slightly between different cybercrimes (for example, Morris and Blackburn, 2009). We focused on cyber-dependent crimes instead of a broader outcome variable that also includes cyber-enabled or cyber-assisted crime. Nevertheless, there may be differences in peer-effects between cyber-dependent crimes as well. We also compared this specific type of cyber-offending with a broad category of traditional offending. As discussed earlier, this addresses the most fundamental research question about differences between cyber-dependent crime and traditional crime in general: the most important step that had to be taken first. Nevertheless, future studies with larger samples and prevalence rates could benefit from comparing both different cyber-dependent crimes and different traditional crimes. In addition to prevalence rate restrictions, our study did not allow for differentiating in the outcome variable because we asked about the online and offline deviance of each social network member only in general, without differentiating between different types of online or offline deviance. A study that used the design of Weerman and Smeenk (2005) might overcome this limitation, because it could directly use self-reported deviant behaviour reported by social ties themselves, instead of having to ask a respondent to indicate the deviance of all social ties separately for a long list of deviant behaviours.

Making a meaningful comparison between less common cyber-dependent crime and traditional crime requires using high-risk samples from the same source, but this sample frame limits the generalizability of our results. Because all respondents were suspected of a crime prior to the 12-month period of the self-report questions, the results reflect the difference in the presence of current deviant social contacts among offenders who have not been deterred by police contact, in comparison with offenders who had not committed crimes in the preceding 12 months. Because our respondents had not been able to avoid 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 affect the IT skill level of offenders, because highly skilled offenders may originate from other countries (for example, European Cybercrime Center, 2014). In other words, the results may be different in the general population, among first offenders and 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 challenge the use of known social processes in interventions against undesirable behaviour in the future, especially if this behaviour moves more and more into the digital world, thereby further reducing connections to the physical world. In sum, this study suggests that underlying theories and established research findings, such as the 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-dependent 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 the suggested future longitudinal comparisons in different samples.

Authors' note

Stijn Ruiter is also affiliated with Utrecht University, The Netherlands.

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This work was supported by the Netherlands Organisation for Scientific Research (NWO) in the framework of the Cyber Security research program under Grant 12-NROI-058b.

Notes

1. Communication with this type of website is completely encrypted and less easy to trace.
2. 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.
3. Results can be requested from the first author.

ORCID iD

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

Supplemental material

Supplemental material for this article is available online.

References

Agnew R (1991) The interactive effects of peer variables on delinquency. *Criminology* 29: 47–72.

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

Blom M, Oudhof J, Bijl RV et al. (2005) Suspected of crime: Non-natives and natives re-examined [Verdacht van criminaliteit: Allochtonen en autochtonen nader bekeken]. *Cahiers*. Heerlen/ Den Haag: CBS/WODC.

Boman JH, Rebellon CJ and Meldrum RC (2016) Can item-level error correlations correct for projection bias in perceived peer deviance measures? A research note. *Journal of Quantitative Criminology* 32: 89–102.

Bossler AM and Burruss GW. (2011) The general theory of crime and computer hacking: Low self-control hackers? In: Holt TJ and Schell BH (eds) *Corporate Hacking and Technology-driven Crime: Social Dynamics and Implications*. New York: Information Science Reference, 38–67.

Chiesa R, Ducci S and Ciappi S (2008) Who are hackers? Part 2. In: Chiesa R, Ducci S and Ciappi S (eds) *Profiling Hackers: The Science of Criminal Profiling as Applied to the World of Hacking*. Boca Raton, FL: CRC Press, 121–188.

De Vries RE and Born MP (2013) The simplified hexaco personality questionnaire and an additional interstitial proactivity facet [De vereenvoudigde hexaco persoonlijkheidsvragenlijst en een additioneel interstitieel proactiviteitsfacet]. *Gedrag & Organisatie* 26: 223–245.

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

Donner CM, Marcum CD, Jennings WG et al. (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) 2014*. The Hague: European Police Office (Europol).

Felson M (1994) *Crime and Everyday Life: Insight and Implications for Society*. Thousand Oaks, CA: Pine Forge Press.

Felson M (1998) *Crime and Everyday Life, Second Edition*. Thousand Oaks, CA: Pine Forge Press.

Goldsmith A and Brewer R (2015) Digital drift and the criminal interaction order. *Theoretical Criminology* 19: 112–130.

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

Grasmick HG, Tittle CR, Bursik RJ et al. (1993) Testing the core empirical implications of Gottfredson and Hirschi's General Theory of Crime. *Journal of Research in Crime and Delinquency* 30: 5–29.

Haynie DL and Kreager DA (2013) Peer networks and crime. In: Cullen FT and Wilcox P (eds) *The Oxford Handbook of Criminological Theory*. Oxford: Oxford University Press, 257–273.

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

Holt TJ (2007) Subcultural evolution? Examining the influence of on- and off-line experiences on deviant subcultures. *Deviant Behavior* 28: 171–198.

Holt TJ (2009) Lone hacks or group cracks: Examining the social organization of computer hackers. In: Schmalleger F and Pittaro M (eds) *Crimes of the Internet*. New Jersey: Pearson Education, 336–355.

Holt TJ and Bossler AM (2014) An assessment of the current state of cybercrime scholarship. *Deviant Behavior* 35: 20–40.

Holt TJ and Kilger M (2008) Techcrafters and makecrafters: A comparison of two populations of hackers. *WOMBAT Workshop on Information Security Threats Data Collection and Sharing, 2008. WISTDCS'08*. Amsterdam: IEEE computer society, 67–78.

Holt TJ, Bossler AM and May DC (2012a) Low self-control, deviant peer associations, and juvenile cyberdeviance. *American Journal of Criminal Justice* 37: 378–395.

Holt TJ, Burruss GW and Bossler AM (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: 31–61.

Holt TJ, Strumsky D, Smirnova O et al. (2012b) Examining the social networks of malware writers and hackers. *International Journal of Cyber Criminology* 6: 891–903.

Hu Q, Xu Z and Yayla AA (2013) Why college students commit computer hacks: Insights from a cross culture analysis. *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: 1–20.

Hutchings A and Clayton R (2016) Exploring the provision of online booter services. *Deviant Behavior* 37: 1163–1178.

Jaishankar K (2009) Space transition theory of cyber crimes. In: Schmalleger F and Pittaro M (eds) *Crimes of the Internet*. New Jersey: Pearson Education, 283–301.

Jansen J, Junger M, Kort J et al. (2017) Victims. In: Leukfeldt ER (ed.) *Research Agenda: The Human Factor in Cybercrime and Cybersecurity*. The Hague: Eleven International Publishing, 45–52.

Kalmijn M (1998) Intermarriage and homogamy: Causes, patterns, trends. *Annual Review of Sociology* 24: 395–421.

Leukfeldt ER, Veenstra S and Stol WP (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: 1–17.

Levi M, Doig A, Gundur R et al. (2017) Cyberfraud and the implications for effective risk-based responses: Themes from UK research. *Crime, Law and Social Change* 67: 77–96.

McCallister L and Fischer CS (1978) A procedure for surveying personal networks. *Sociological Methods & Research* 7: 131–148.

McGuire M and Dowling S (2013) Chapter 1: Cyber-dependent crimes. In: *Cyber Crime: A Review of the Evidence*. Home Office Research Report 75, 4–34.

McPherson M, Smith-Lovin L and Cook JM (2001) Birds of a feather: Homophily in social networks. *Annual Review of Sociology* 27: 415–444.

Marcum CD, Higgins GE, Ricketts ML et al. (2014) Hacking in high school: Cybercrime perpetration by juveniles. *Deviant Behavior* 35: 581–591.

Morris RG (2011) Computer hacking and the techniques of neutralization: An empirical assessment. In: Holt TJ and Schell BH (eds) *Corporate Hacking and Technology-driven Crime: Social Dynamics and Implications*. New York: Information Science Reference, 1–17.

Morris RG and Blackburn AG (2009) Cracking the code: An empirical exploration of social learning theory and computer crime. *Journal of Crime and Justice* 32: 1–34.

National Cyber Security Centre (2012) Cybercrime: From recognition to report [Cybercrime. Van herkenning tot aangifte]. NCSC [Nationaal Cyber Security Centrum], Ministry of Security and Justice.

Pratt TC, Cullen FT, Sellers CS et al. (2009) The empirical status of social learning theory: A meta-analysis. *Justice Quarterly* 27: 765–802.

Rogers MK (2001) A social learning theory and moral disengagement analysis of criminal computer behavior: An exploratory study. PhD thesis, University of Manitoba. URL (accessed 25 April 2019): https://www.cerias.purdue.edu/assets/pdf/bibtex_archive/rogers_01.pdf.

Rokven JJ, Boer GD, Tolsma J et al. (2017) How friends' involvement in crime affects the risk of offending and victimization. *European Journal of Criminology* 14: 697–719.

Rokven JJ, Tolsma J, Ruiter S et al. (2016) Like two peas in a pod? Explaining friendship selection processes related to victimization and offending. *European Journal of Criminology* 13: 231–256.

Royston P (2004) Multiple imputation of missing values. *Stata Journal* 4: 227–241.

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

Sampson RJ and Laub JH (1993) *Crime in the Making: Pathways and Turning Points Through Life*. Cambridge, MA: Harvard University Press.

Soudijn MRJ and Zegers BCHT (2012) Cybercrime and virtual offender convergence settings. *Trends in Organized Crime* 15: 111–129.

StataCorp (2017) Mi test – test hypotheses after mi estimate. *Multiple-imputation Reference Manual*, 15th edn. Texas: Stata Press, 328–336.

Steinberg L and Monahan KC. (2007) Age differences in resistance to peer influence. *Developmental Psychology* 43: 1531–1543.

Suler J (2004) The online disinhibition effect. *CyberPsychology & Behavior* 7: 321–326.

Sutherland EH (1947) *Principles of Criminology, 4th ed*. Oxford, England: J. B. Lippincott.

Svensson R, Weerman FM, Pauwels LJR et al. (2013) Moral emotions and offending: Do feelings of anticipated shame and guilt mediate the effect of socialization on offending? *European Journal of Criminology* 10: 22–39.

Van Gelder J-L and De Vries RE (2012) Traits and states: Integrating personality and affect into a model of criminal decision making. *Criminology* 50: 637–671.

Von Hippel PT (2007) Regression with missing ys: An improved strategy for analyzing multiply imputed data. *Sociological Methodology* 37: 83–117.

Wall DS (2001) Cybercrimes and the internet. In: Wall DS (ed.) *Crime and the Internet*. London: Routledge, 1–17.

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

Weerman FM and Smeenk WH (2005) Peer similarity in delinquency for different types of friends: A comparison using two measurement methods. *Criminology* 43: 499–524.

Weulen Kranenbarg M, Holt TJ and Van Gelder J-L (2017a) Offending and victimization in the digital age: Comparing correlates of cybercrime and traditional offending-only, victimization-only and the victimization-offending overlap. *Deviant Behavior* 1–16.

Weulen Kranenbarg M, Van Der Laan A, De Poot C et al. (2017b) Individual cybercrime offenders. In: Leukfeldt ER (ed.) *Research Agenda: The Human Factor in Cybercrime and Cybersecurity*. The Hague: Eleven International Publishing.

Yar M (2005) The novelty of ‘cybercrime’. An assessment in light of routine activity theory. *European Journal of Criminology* 2: 407–427.

Yar M (2013) Cybercrime and the internet, an introduction. In: Yar M (ed.) *Cybercrime and Society*, 2nd edn. London: Sage, 1–20.

Young JTN and Rees C (2013) Social networks and delinquency in adolescence: Implications for life-course criminology. In: Gibson CL and Krohn MD (eds) *Handbook of Life-course Criminology: Emerging Trends and Directions for Future Research*. New York: Springer, 159–180.

Young JTN, Rebellon CJ, Barnes JC et al. (2014) Unpacking the black box of peer similarity in deviance: Understanding the mechanisms linking personal behavior, peer behavior, and perceptions. *Criminology* 52: 60–86.