Marleen Weulen Kranenbarg

# Cyber-offenders versus traditional offenders

## An empirical comparison

# Chapter 6

## General conclusion and discussion

## 6.1 Introduction

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



## 6.2 General results

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

### *6.2.1 Longitudinal life-course study (Chapter 2)*

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

With respect to professional life circumstances, the results were more in line with the expectations. There was no statistically significant effect of employment or enrolment in education on cyber-offending, while these life circumstances did

reduce traditional offending statistically significantly. Within the complete offender population of this study, the results even pointed to some interesting differences between general employment and employment in the IT-sector and enrolment in education. In line with the estimates for traditional crime, general employment reduced the likelihood of cyber-offending. In contrast, employment in the IT-sector increased the likelihood of cyber-offending. Similarly, being enrolled in education, both general- and IT-education, also increased the likelihood of cyber-offending. These results regarding personal and professional life circumstances seem to indicate that, even though cyber-offending is less visible than traditional offending, social control of others can reduce the likelihood of cyber-offending. However, some traditionally protective life circumstances can increase opportunities for cyber-offending and apparently the control of others in these situations cannot prevent a person from using those opportunities to commit cybercrime.

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

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

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

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

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

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



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

### *6.2.4 Clusters of offences and related motivations (Chapter 5)*

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

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

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

### *6.2.5 General conclusion*

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

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

plan and execute their crimes. Similarly, intrinsic motivations, like curiosity and the educational aspect of learning IT-skills through offending, distinguish cyber-offending from traditional offending.

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

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



## 6.3 General limitations

Each empirical chapter discussed the limitations that were related to the data and measures for that specific domain. Nevertheless, some general limitations should be addressed here. First of all, the samples in this dissertation were drawn from

police and prosecutor's data. For the longitudinal dataset of Chapter 2, this means that the outcome variable reflects when a person was a suspect of a crime, but it is unknown if this person was actually guilty of committing that crime and it is unknown to what extent this person also committed crimes in the years he or she was not caught by the police. For Chapter 3 to 5, this means that the population that was studied is a high risk population. The analyses indicated which present-day risk factors, social contacts and motivations were related to present-day self-reported offending of people who had been caught by the police for committing a crime in the past, prior to the twelve-month period of the self-report questions.

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

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

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

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



## 6.4 Future research

Each chapter already discussed some future research directions for the specific domain addressed in that chapter. However, several general directions are important to discuss here. First of all, to address the general limitations discussed

above, replication in future research in different and larger samples, preferably with in-depth longitudinal data, is necessary. Different samples may include non-Dutch, general population, or high risk samples of juveniles or adolescents. To enhance the generalisability of research based on police data samples, it could also be informative to study the differences between cyber-offenders who have been caught and cyber-offenders who have been able to avoid apprehension. This could, for example, shed light on the question to what extent they differ in their motivations to commit cybercrimes.

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

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

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

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



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

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

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

## 6.5 Practical implications

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

When using interventions designed for traditional offenders, empirically identified differences and similarities between cyber-offenders and traditional offenders should be kept in mind. It is not advisable to base the application of traditional interventions to cybercrime purely on hypothetical similarities. For example, this dissertation indicated that, in contrast to hypotheses in the literature, cyber-offenders differ from white-collar offenders with respect to their motivations for committing crimes. While financial motivations are by far the most important motivation for white collar crimes, these motivations are almost absent for cyber-offences in this sample. Therefore, interventions for cybercrime may not benefit much from reducing the expected financial gain of committing cybercrimes. In contrast to traditional crime, but in line with previous cybercrime research, this dissertation has shown that the level of IT-skills is an important predictor of cyber-

offending, both when measured subjectively or with an objective IT-skills test. Cyber-offenders even indicated that they mainly commit their crimes out of curiosity and for the educational aspect of enhancing their IT-skills. Therefore, interventions may benefit from stimulating them to satisfy these needs in legitimate ways, as this may reduce their need for using and enhancing their skills in an illegal way.

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



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

Another way of increasing the risk perception of offenders is by so-called 'cease and desist visits' (National Crime Agency, 2017b). These may be a useful tool in preventing further and more serious offending of known offenders. In these 'cease and desist visits' an offender whose behaviour is not serious enough for arrest, has a face-to-face visit with a police officer. This visit shows that the offender's criminal behaviour does not go undetected and the offender is advised to desist from committing crimes in the future, to prevent arrest and other negative consequences. However, as discussed above, it is very important that this type of

intervention also provides guidance in how to move from illegal use of IT-skills to responsible use of IT-skills. In addition, it is important that continuing offending after such a visit will actually result in a punishment. Otherwise, these visits will lose their impact in the future.

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

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

Lastly, in an attempt to reduce the prevalence of cybercrime in the future, young people should not only learn IT-skills, but also responsible ways of using those skills. Right now, general prevention programs against cybercrime generally focus on techniques to prevent victimisation and, for example, schools start including programming and other IT-skills in their educational program. These general prevention programs are important to increase resilience against cyberattacks in the future, but ethics and other aspects of responsible IT-use should be an important component of these programs as well. Otherwise, young people will learn IT-skills without learning how to use them responsibly. Educational institutes

already adopted several ways of addressing their students' offline risk behaviour and they should now adopt their strategies to behaviour in the digital world as well. In that way educational programs may be able to reduce their students offending in the present, and maybe even provide them with the skills and ethics that could reduce the prevalence and impact of new types of cyber-dependent offending that will arise in the future.

# References

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Office for National Statistics. (2015). Improving Crime Statistics in England and Wales. *Crime Statistics, Year Ending June 2015 Release*. Retrieved from http://webarchive.nationalarchives.gov.uk/20160105160709/http://www.ons.gov.uk/ons/rel/crime-stats/crime-statistics/year-ending-june-2015/sty-fraud.html.

Ousey, G. C., Wilcox, P., & Fisher, B. S. (2011). Something Old, Something New: Revisiting Competing Hypotheses of the Victimization-Offending Relationship among Adolescents. *Journal of Quantitative Criminology, 27*(1), 53-84.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Svensson, R., Weerman, F. M., Pauwels, L. J. R., Bruinsma, G. J. N., & Bernasco, W. (2013). Moral Emotions and Offending: Do Feelings of Anticipated Shame and Guilt Mediate the Effect of Socialization on Offending? *European Journal of Criminology, 10*(1), 22-39.

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

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

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

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

Turanovic, J. J., & Pratt, T. C. (2013). The Consequences of Maladaptive Coping: Integrating General Strain and Self-Control Theories to Specify a Causal Pathway between Victimization and Offending. *Journal of Quantitative Criminology, 29*(3), 321-345.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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