nscr

Understanding cybercriminal behaviour among young people

Results from a longitudinal network study among a relatively high-risk sample

Marleen Weulen Kranenbarg
Yaloe van der Toolen
Frank Weerman

Amsterdam, 2022

Nederlands Studiecentrum
Criminaliteit en Rechtshandhaving

VU VRIJE UNIVERSITEIT AMSTERDAM

Understanding cybercriminal behaviour among young people

Results from a longitudinal network study among a relatively high-risk sample

Marleen Weulen Kranenbarg
Yaloe van der Toolen
Frank Weerman

January, 2022

This work was supported by the UK Home Office through a National Cyber Security Programme research grant

VU UNIVERSITY AMSTERDAM
nscr Netherlands Institute for the Study of Crime and Law Enforcement

Please cite this report as:
Weulen Kranenbarg, M., Van der Toolen, Y., & Weerman, F. (2022). *Understanding cybercriminal behaviour among young people: Results from a longitudinal network study among a relatively high-risk sample.* Amsterdam: VU University Amsterdam/Netherlands Institute for the Study of Crime and Law Enforcement.

Contents

Acknowledgements

Many individuals and organisations have been important for conducting this study. Most importantly, we could not have done this research without the schools and the students who participated in this study. We would like to thank all the schools for spending their valuable time on our project, and our participants for their, often enthusiastic, participation. We would also like to thank the UK Home Office for funding this project and our Home Office contact persons for their advice and flexibility during the process. In addition, we would like to thank the experts who participated in our expert meeting and who provided the valuable insights and implications that really helped us to translate our results into practical implications. Lastly, we would like to extend our thanks to the various colleagues who advised us on data collection and analyses and on interpreting our results. We are grateful to them all for their helpful suggestions.

Executive summary

This report aims to increase our insight into the explanation of cyber-delinquency among juveniles. We examined which individual characteristics and environmental factors are related to different types of cybercrime, with a specific focus on the importance of peer relationships. We used a longitudinal research design (three waves of data collection) among a substantial sample of Dutch youths in secondary or tertiary education (with ages between 12 and 25), who were following ICT programmes, tracks, or courses. These students were chosen because they are considered to be at an elevated risk of committing cybercrime. We used questionnaires to collect self-report data on a large variety of cyber-offences, and on characteristics of both offline and online peers. We distinguished between cyber-dependent offending (i.e. offences requiring the use of online means) and cyber-enabled offending (i.e. offences existing in the offline world, but that can also be conducted online). We also included questions about common traditional types of offending. In addition, we asked the respondents about various individual characteristics and environmental factors and we collected detailed social network data on the respondents' school friends. Our methods (for details, see Chapter 3) addressed various important limitations in previous research on cyber-delinquency (see Chapter 2).

A substantial proportion of our respondents were involved in at least one of the various types of cyber-dependent and cyber-enabled crime. The juveniles in our sample reported even more often cyber-delinquency than traditional delinquency (see details in Chapter 4). Of all the participating juveniles, between 45% (in wave 2) and 51% (in wave 1) indicated they had committed a cyber-dependent offence, while 35-39% had committed a cyber-enabled offence. The most prevalent cyber-dependent offences were hacking by guessing a password (24-25%), stealing (illegally copying) files or data (22-23%), and vandalising (modify or delete) data (17-19%). More technical cyber-dependent offences, such as hacking by using technical applications (11-12%) or exploits (12-16%), were also quite common in this high-risk sample. The most prevalent cyber-enabled offences were fighting out conflicts online (22-33%) and online fraud (6-15%).

Cyber-dependent offences were related mainly to individual factors, while cyber-enabled and traditional offences were also related to the environmental factors included in this study. The table below summarises the characteristics and factors that are statistical significantly related to the three investigated types of offending (for details about their content and measurement, see Chapter 3). The elements in green are significantly positively related to a particular type of offending, while the ones in red are significantly negatively related. In else, the green factors increase the probability of a particular type of offending, and the red factors decrease this probability. Most of the found risk factors are in line with what has been found in previous research on (often adult) cybercrime offenders. The finding that low self-control is related to both categories of cyber-delinquency is not in line with a few studies that suggested that high self-control is needed to conduct more the more technical types of cybercrime. This may be explained by the already high levels of ICT knowledge among the respondents of our study.

Cyber-dependent delinquency	Cyber-enabled delinquency	Traditional delinquency
INDIVIDUAL FACTORS		
- Age	- Age	- Age
+ Low self-control	+ Low self-control	+ Low self-control
+ Good social skills	+ Good social skills	+ Good social skills
+ Computer addiction	+ Computer addiction	+ Computer addiction
+ ICT knowledge		- ICT knowledge
+ Positive cyber-behaviour	+ Positive cyber-behaviour	+ Positive cyber-behaviour
ENVIRONMENTAL FACTORS		
		- Offline rules by parents
	+ Home alone	
		- Online rules by school
	- School satisfaction	- School satisfaction
	+ ICT education satisfaction	+ ICT education satisfaction

Red (-) = negative significant effect; green (+) = positive significant effect.

Overall, the findings suggest that the factors leading to cyber-enabled offending are more similar to traditional offending than those leading to cyber-dependent offending. For cyber-dependent delinquency, ICT knowledge seem to be more important than for cyber-enabled delinquency, and gaming is also related to this type of offending, although not very strongly. More importantly, environmental factors such as being home alone and school satisfaction, seem to be unrelated to cyber-dependent delinquency while they are associated with the

level of cyber-enabled delinquency. This lack of a relationship for cyber-dependent delinquency implies that it is also more difficult to focus intervention or prevention efforts on parents and schools to counteract this type of behaviour. Details on the interpretation of each result can be found in Chapter 4.

A surprising overlap was found between cyber-delinquent behaviour and positive cyber-behaviour, indicating that differentiating between 'good' and 'bad' students may not be as easy as it may seem. We also found both types of cyber-offending, as well as traditional offending, were related to having better social skills. Whilst it seems counter intuitive that these more positive characteristics were associated with more offending, it may also imply that rule breaking is not as black and white as it seems. There may be an underlying tendency among students with more social skills to be more active online, and this can result both in cyber-offending and in online activities that are intended to be beneficial to others. Both positive and negative cyber behaviour may be challenging to students following ICT education. This finding has implications for interventions, and suggest that students might be diverted towards choosing positive alternatives to offending (see Chapter 4).

Respondents often underestimate the involvement of their friends in cyber-delinquency, particularly in the case of cyber-dependent delinquent behaviour. In about half of the cases, respondents were not aware of the actual cyber-delinquent behaviour of their school friends (for details, see Chapter 5).

Perceptions of friends' cyber-delinquency were more strongly related to an individual's own cyber-delinquency than friends' actual self-reports of delinquency. This suggests that young people have a tendency to adapt their cyber-behaviour to how they *believe* their friends behave rather than to how these friends actually behave. It may also mean that young people think that there friends are more like themselves than they really are (for details, see Chapter 5).

Perceptions about the cyber-delinquency of *online* friends were equally strongly related to individual cyber-delinquency as perceptions about cyber-delinquency of *offline* friends. By contrast, perceptions of offline friends' traditional delinquency were relatively more strongly related to individual traditional delinquency than the perceptions about online friends (see Chapter 5). This suggests that perceptions about online friends may have a relatively more important role for cyber-delinquency than for traditional offending.

It remained unclear as to what causes short-term changes among respondents (over a six-months period) in the level of cyber-delinquent behaviour. With regard to friends, no clear indications were found for direct influence effects of actual reported offending by school friends. The network analyses also did not show that cyber delinquency was important in the selection of school friends. In general, respondents chose their friends based either on gender or on general network mechanisms (e.g. choosing friends of friends, or selecting the more popular students). Traditional types of delinquency appeared potentially important as criteria for selecting friends, but cyber-delinquency did not (at least within schools; see further details in Chapter 6).

Our findings can be useful to further develop different types of measures to address cyber delinquency. These measures may be focused on preventing cyber offending in the general population (primary prevention), activities targeted at relatively 'high-risk' groups (secondary prevention), and interventions directed at reducing recidivism for juveniles already involved in substantial levels of cyber-delinquency (tertiary prevention). General measures may be most useful if they focus on relatively high risk groups, such as ICT students who have relatively high rates of self-reported involvement in cyber delinquency. In the case of cyber-dependent crime, these prevention and intervention measures could benefit most from focussing on individual factors such as computer addiction, since for this type of cyber offending no relationships were found with environmental factors. In the case of cyber-enabled crime, interventions could also address factors at home and in schools that are related to this type of offending. These interventions should be tailored to individual needs, given that different groups of offenders may be identified, and motivations and ICT skill levels may also differ substantially (see Chapter 7).

Schools may be able to help in the prevention of cyber-offending early in a criminal career. General school efforts to increase school satisfaction among their students can also be beneficial to prevent involvement in cyber-delinquency. More specifically, schools may spot early signs of potential cyber-delinquency in their students and develop measures to act on these signs. Additionally, while school rules alone do not seem to have an inhibiting effect on cyber-delinquency, schools may have the potential to encourage positive cyber-behaviour. The overlap we found between positive and negative cyber-behaviour suggests that schools could provide lessons on the distinction between 'good' and 'bad' cyber-behaviour and, in this way, encourage their students to choose the positive alternative (see Chapter 7).

Parents may play a role in preventing cyber-delinquency, especially cyber-enabled offences. Increasing online rules by parents and reducing time spent alone at home may reduce cyber-enabled delinquency. However, parents may need some help in how to prevent their children's online delinquency. Schools could involve parents in programmes aimed at prevention, raise awareness among parents and offer them suggestions on how to make online rules and supervise children's online behaviour (see Chapter 7).

Prevention and intervention measures should not only target school friends (and perceptions about school friends), but also other types of friendships (and perceptions about these types of friendship). Unlike traditional delinquency, perceptions about different types of friends seem to be equally important (see Chapter 7). If juveniles think that their friends are involved in cyber delinquency or when they become aware that this is actually the case, it is important to be resistant against peers and group influences and not see cyber-delinquent peers as role models.

Our study has its limitations, which should be kept in mind when interpreting the results. Firstly, the results may not be generalisable to young people in this age group in general, as our study sampled a group of Dutch juveniles with a relatively high-risk of cyber-offending. Secondly, we did not differentiate between less serious and more serious forms of cyber-offending; instead we grouped the different types of cyber-offending into two general categories that are distinguished in the literature (cyber-dependent and cyber-enabled offending). Thirdly, time constraints meant we could only include a selection of the most

frequently mentioned individual and environmental variables from the literature on cyber-offending, while cyber-delinquency may also be related to other factors, which were not measured. Fourthly, as our measures of actual self-reported delinquency of peers were limited to school friends, we could not investigate differences between actual self-reported and perceptual measurements of friends' delinquency for offline out-of-school and online networks of respondents' friends. For more details and suggestions on how to address the limitations in future research, see Chapter 7.

In summary, our results suggest that prevention and intervention measures should address various factors simultaneously and distinguish between specific groups of offenders and their needs. Schools and parents (in addition to formal preventive organisations, such as the police and probation services) may play an important role in preventing and reducing negative cyber-behaviour, and also in encouraging positive cyber-behaviour (see Chapter 7).

1. Introduction

1.1 Background

A substantial part of UK society falls victim to cybercrime every year. Recent figures from the Telephone-operated Crime Survey for England and Wales show that, in the year ending September 2020, an estimated 1.7 million incidents of computer misuse were experienced by adults (i.e. persons aged 18 and over) in England and Wales (ONS, 2021). Moreover, over half (53%) of fraud incidents experienced by adults in England and Wales in the year to March 2020 involved the internet or online activity (ONS, 2020). These numbers indicate that cybercrime poses a big challenge to the UK, and this can easily be extended to modern societies in general.

Nowadays, cybercrime also accounts for a substantial share of juvenile delinquency. In 2016, Dutch self-report research estimated that 31% of young people had committed at least one cyber-offence in the previous year. This is a substantial number, and very comparable to the prevalence of traditional offences among youths (35%; see Van der Laan & Goudriaan, 2016). In the UK, research conducted by the National Crime Agency indicated that many cyber-offenders start their illicit computer activities at a young age (National Crime Agency, 2017). This indicates that cyber-offending is also an important component of UK juvenile delinquency.

Recent criminological studies have increasingly focused on identifying explanations for individual cyber-offending (for recent overviews, see Holt & Bossler, 2014; Leukfeldt, 2017; Leukfeldt & Holt, 2020). Since many forms of cybercrime can only take place in an anonymous digital context and the circumstances in which they take place are less bound to fixed places and times than traditional types of crime, the question arises as to what extent traditional criminological insights are helpful for explaining and targeting cybercrime (see, for example, Grabosky, 2001; Weerman, 2019; Yar, 2005). However, whereas criminological knowledge regarding traditional delinquency is well developed, empirical research on cyber-offending is still scarce (see, for example, Leukfeldt & Holt, 2020). This means that it is still unclear as to what extent existing insights into traditional juvenile delinquency and the development of traditional criminal careers can be extended to the digital context.

The UK National Cyber Security Strategy 2016-2021 emphasised that a further understanding of cyber-offenders and their criminal careers is crucial for the developmentment of Prevent approaches that could deter young people from becoming involved in cybercrime (H.M. Government, 2016). In line with this, the Home Office commissioned research on this topic (UK Home Office, 2018).

1.2 Focus of the current study

This report focuses on cyber-offending among young people. Cyber-offending covers a wide range of online offences, ranging from simple to very advanced offences, and from extensions of existing offences to brand new opportunities to commit crime. Throughout our analyses, we distinguished between cyber-dependent, cyber-enabled and traditional offences. Cyber-dependent offences can only be committed online and require ICT systems; cyber-enabled offences are types of crime that also exist offline, but make use of ICT systems; traditional offences are offline acts such as theft, vandalism and violence (McGuire & Dowling, 2013b, 2013a). In our analyses, we examined which individual characteristics and environmental factors are related to these three categories of offending.

We focused specifically on the role of different types of peer relationships with regard to cyber-offending. The role of peers is a well-studied topic in criminology research on traditional offending. Delinquent juveniles often have (or believe they have) friends who themselves also engage in delinquent behaviour (see, for example, Agnew, 1991; Haynie, 2001, 2002; Weerman, 2011). This finding has been linked to various criminological theories and led to a stream of empirical studies focusing on unravelling the different processes and mechanisms through which peers play a role in traditional delinquency (Akers, 1998; Hoeben, Meldrum, Walker, & Young, 2016; Pratt et al., 2010; Sutherland, 1947; Warr, 2002). Recent studies have shown that offenders committing cybercrimes also often have cyber-delinquent friends (see, for example, Holt, Bossler, & May, 2012; Holt, Burruss, & Bossler, 2010; Marcum, Higgins, Ricketts, & Wolfe, 2014; Morris & Blackburn, 2009; Rogers, 2001; Skinner & Fream, 1997; Weulen Kranenbarg, Ruiter, & Van Gelder, 2021). However, the relative novelty of cyber-offending means that much is still unknown about the role played by peers in cyber-delinquency.

It is unclear, for example, as to what extent cyber-offenders are truly similar to their peers, or whether they merely *think* they are. All previous studies on the role of peers in cyber-offending have relied on perceptual (i.e. indirect) measures of the delinquency of friends, based on questions in which respondents were asked about their *perceptions* of their friends' delinquency levels. However, research on traditional delinquency suggests that individuals tend to overestimate the extent to which the delinquency levels of their friends match their own delinquent behaviour (Boman, Rebellon, & Meldrum, 2016; Weerman & Smeenk, 2005).

It is also still unclear whether and to what extent cyber-delinquent offenders exert *influence* on the behaviour of their friends. Until now, no longitudinal studies on the relationship between individual and peer cyber-offending have been conducted. Previous studies were consequently unable to provide sufficient insight into the dynamic processes behind the observed peer similarity in cyber-delinquent behaviour. Is this finding reflective of adolescents who are *influenced* by their peers in committing cyber-offences, or does it mean that cyber-delinquents *select* friends who are also involved in these type of offences?

Lastly, it is unclear how *online* peers affect individual cyber-delinquency compared to *offline* peers. Previous research on cyber-delinquent behaviour has devoted very little attention to the role of online friends in comparison to offline friends. This is problematic, given that indications suggest that friends and contacts from online forums play an important role in the exchange of knowledge and opportunities for committing cyber-offences (Holt, 2007; Hutchings, 2014).

In addition to this specific focus on the role of peer relations, we also aim to provide insights into the main personal characteristics and social context of juveniles who are involved in cyber-delinquency. By doing so, we will provide an initial base for understanding how cyber-delinquency develops among juveniles. This will also enable us to put our findings about the role of peers into perspective. Our analyses will include risk factors that are already known to be related to law-breaking in general, as well as assets and skills that make it easier for young people to commit cyber-offences. It has been argued that committing more advanced types of cybercrimes requires good knowledge and practical skills about the possibilities and peculiarities of the internet (Holt, 2013; Holt & Kilger, 2012; McGuire & Dowling, 2013a; Weulen Kranenbarg, Holt, & Van Gelder, 2019), and we want to scrutinise the extent to which juvenile cyber-delinquents possess such skills to a greater extent than other juveniles.

Additionally, we will investigate the extent to which online and offline rules imposed by parents or schools are related to cyber-offending.

Our study aims to contribute to intervention and policy measures, in particular to Prevent approaches first initiated by the National Cyber Security Strategy 2016-2021. Prevention and intervention measures and programmes may benefit from our insights on how young people's social ties influence cyber-offending and which type of peer relations should be targeted. At the end of this report, therefore, we will formulate the main implications of our findings for practices and policies to address cybercrime.

1.3 Aim and research questions

This study aims to increase our insights into explanations for cyber-delinquency, in particular by scrutinising the role of different types of peers in different types of cyber-delinquent behaviour by young people. It also examines other major individual characteristics and environmental factors potentially related to cyber-delinquency that have been identified in the literature. In the following chapters, we focus on the following research questions:

1. How are different types of cyber-delinquent behaviour among young people related to major individual characteristics and environmental factors?
2. How is cyber-delinquent behaviour among young people related to actual and perceived cyber-delinquent behaviour of offline and online peers?
3. What is the causal relationship between actual cyber-delinquent behaviour of young people and that of their peers?
4. To what extent do these results differ between cyber-dependent, cyber-enabled and traditional delinquent behaviour?
5. How can we translate our findings into practice and policy implications?

1.4 General approach

In order to answer our research questions, we conducted a longitudinal study (three waves) among a substantive sample of young people (aged 12 – 25) who were considered to be at an elevated risk of committing cyber-offences: ICT students, and students in general forms of education who were following ICT tracks or courses. We collected self-report data on a large variety of cyber- and traditional offences, and also asked respondents to report on the cyber-offending and traditional offending levels of their offline and online peers. We also collected data on various individual characteristics and environmental factors, as well as detailed social network data on the respondents' school friends. These data enabled us to employ advanced longitudinal network analysis (stochastic actor-oriented models; see Snijders, 2001; Snijders, Van de Bunt, & Steglich, 2010; Steglich, Snijders, & Pearson, 2010). By using this method we could investigate whether and how cyber-delinquent behaviour of individuals' friends is causally related to the cyber-delinquent behaviour of the individuals themselves. Data collection took place in the Netherlands, between September 2019 (wave 1) and June 2020 (wave 3).

Our approach made it possible to target limitations from previous studies on peers and cyber-delinquency. First, by applying a longitudinal social network method, we could more effectively study causal relationships and distinguish between different social processes. Second, the current study measured actual peer delinquency directly by using social network data in addition to the commonly used perceptual measures of peer delinquency that rely on adolescents' perceptions about offending behaviours of their peers. This enabled us to arrive at less biased effect estimates of the effects of peers' actual cyber-behaviour on individual offending. Third, we were able to study the role in cyber-delinquency played by different types of friends: school friends, friendships existing outside school, and friendships existing exclusively online. Fourth, we collected detailed information about the ICT skills of respondents in addition to personal and environmental risk factors that are known from research on traditional forms of delinquency. Finally, by focusing on cyber-dependent, cyber-enabled and also traditional offences, this report will provide insights in the extent to which the dynamics pertaining to these types of offences differ.

By specifically targeting these limitations, we hope to provide meaningful insights for practice and policy, and for the further development of successful measures aimed at preventing and deterring young people from becoming involved in cybercrime.

1.5 Reader's guide

The outline of this report is as follows:

Chapter 2 provides a brief overview of the *literature* on the role of peers in cyber- and traditional delinquency, and on the processes of influence and selection. Chapter 3 describes our *research methods*. First we describe the sampling of students, the development of the questionnaire and the operationalisation of the main variables. Next, we give a short overview of our analytical methods.

The subsequent chapters present our empirical research findings. Chapter 4 describes the *prevalence of cyber-delinquency* in the high-risk sample used for this research. We also explore the relationship between cyber-behaviour and a large variety of *individual characteristics* and *environmental risk factors*. Chapter 5 investigates the extent to which the relationship between individual offending and *perceived cyber-delinquent behaviour of friends* (indirect measures) differs from the relationship between individual offending and *actual cybercriminal behaviour of friends* (direct measures). This chapter also examines the role of *different types of friends* in individual cyber-offending. Chapter 6 analyses different *causal processes* responsible for the relationship between actual cybercriminal behaviour of friends and someone's own cybercriminal behaviour. By using longitudinal social network methods, we investigate the extent to which selection and influence effects play a role.

Chapter 7 presents the conclusions and the implications of our findings. In this final chapter, we reflect on the insights from the previous chapters, and discuss *conclusions and implications for prevention and intervention measures*. We combine this with insights gained from our discussions with practitioners and policymakers during our *expert meeting*.

2. Theory and research on the role of peers in delinquent behaviour

2.1 Introduction

One of the most replicated findings in research on traditional forms of delinquency is that young people who engage in delinquent behaviour are likely to have friends who also engage in delinquent behaviour (see, for example, Agnew, 1991; Akers, 1998; Haynie, 2001, 2002; Pratt et al., 2010; Sutherland, 1947; Warr, 2002; Weerman, 2011). Criminology has offered two general explanations for this observation. The *influence* perspective emphasises processes of social learning, and states that friends influence each other in delinquent behaviour through the adoption of deviant definitions and processes such as imitation and reinforcement (Akers, 1973, 1998; Sutherland, 1947). According to the *selection* perspective, on the other hand, delinquent individuals either consciously or unconsciously initiate friendships with each other and thus select each other as friends (Glueck & Glueck, 1950; Gottfredson & Hirschi, 1990; Hirschi, 1969). Whereas influence and selection were originally perceived as opposing explanations, it is now generally agreed that both processes are important for delinquent behaviour (Gallupe, McLevey, & Brown, 2018; Warr, 2002).

2.2 Influence processes

The influence perspective emphasises the processes through which friends can *influence* each other in their behaviour and encourage delinquent behaviours. The classic theoretical foundation for this perspective can be found in Sutherland's differential association theory (Sutherland, 1947), which states that social interaction with delinquent people and delinquent settings enhances the likelihood that individuals will take over delinquent knowledge and attitudes and engage in delinquent behaviour themselves. Sutherland's work has been extended into social learning theory by Akers (1973), who distinguished several psychological mechanisms that might be responsible for this behavioural assimilation. In line with Sutherland's differential association theory, Akers, too, argued that interacting with delinquent friends may lead to delinquent attitudes being adopted. In addition, he specified various social learning processes contributing to this. One of these processes is social reinforcement, which occurs when delinquent acts are positively evaluated by others and

rewarded with acceptance and social status. In this way, transgressive acts are encouraged by the delinquent peer group, whereas socially desirable behaviour can be disapproved. An additional process that is distinguished in social learning theory is imitation, which occurs when a person copies the behaviour of someone else who seems to be rewarded for his or her delinquent behaviour. Imitation may lead to the initiation of delinquency, while reinforcement can be seen as crucial for continuing delinquent behaviour.

The influence mechanisms distinguished by Akers in social learning theory have been studied extensively in criminology. A meta-analysis of 133 social learning theory studies found a strong relationship between differential association (i.e. having delinquent friends) and delinquent behaviour in particular. However, evidence for reinforcement and imitation is less consistent (Pratt et al., 2010).

Some theorists suggest that it is not so much *delinquent* friends, but hanging around unsupervised in peer groups in general that influences individuals to engage in delinquent behaviour. Osgood and Anderson (2004), for example, argued that taking part in unstructured activities with peers – such as hanging around on the street, driving around in a car, or going to parties – without adult supervision results in opportunities and temptations for delinquent behaviour. Warr (2002) argued that general group processes among adolescents, such as fear of ridicule, can also lead to delinquent behaviour. Warr states that peer groups can induce individual engagement in illegal activities not primarily because these individuals want to be liked, but because they want to avoid being rejected by the group. In his view, other factors such as loyalty (e.g. not 'betraying' your friends, or engaging in illegal activities together to solidify the friendship) and obtaining status are also important explanations for delinquent behaviour.

2.3 Selection processes

The selection perspective emphasises the role of delinquent behaviour as one of the factors and conditions determining which friendship ties are formed (or, reversely, are broken). One of the processes underlying this perspective is *homophily*: people are more likely to associate with each other when they have similar characteristics (Lazarsfeld & Merton, 1954;

McPherson, Smith-Lovin, & Cook, 2001). As similarities between people can occur in various forms, people may select others based multiple characeristics..

Firstly, general characteristics such as age, gender and ethnicity can be important in friendship selection processes. Previous research has indicated that children are more likely, for instance, to pick friends with the same gender (Shrum, Cheek, & Hunter, 1988) or ethnicity (Baerveldt, Van Duijn, Vermeij, & Van Hemert, 2004) as themselves.

Secondly, preferences related to the formation of social networks in general can also play a role in friendship formation. People tend, for instance, to reciprocate friendships (see, for example, Burk, Steglich, & Snijders, 2007). Further they also tend to become friends with the friends of their friends, a process known as transitivity (see, for example, Davis, 1970).

Thirdly, people's attitudes and salient behaviours can play an important role in friendship selection (see, for example, Kandel, 1978). These may include political views, moral attitudes, substance use and all sorts of conforming and deviant behaviour. Early studies on crime found that delinquent individuals more often engage in friendships with people who are also delinquent themselves (Glueck & Glueck, 1950; Hirschi, 1969). This may reflect a mental preference for having friends with similar behaviour (or other characteristics related to that behaviour). However, it could also reflect more instrumental considerations. For instance, it could be beneficial for delinquents to be friends with each other so that they can share information or tools that come in handy when pursuing criminal opportunities (Rokven, Tolsma, Ruiter, & Kraaykamp, 2016; Wasserman & Galaskiewicz, 1994).

Engaging in criminal behaviour can also lead to another process that is relevant for friendship selection and network formation: spending time in certain locations. There are indications that specific social contexts can serve as *offender convergence settings*: physical locations, such as shady bars or gambling facilities, that particularly attract offenders (Felson, 2003). Offenders tend to congregate at these locations to relax or make deals. These locations offer a social environment that provides offenders with new opportunities to interact and form friendship ties with other offenders (Steglich et al., 2010). In recent years, some attention has also been devoted to *virtual* offender convergence settings (Soudijn & Zegers, 2012). These are virtual locations, such as online forums devoted to illicit online activities, where potential cyber-offenders can meet and exchange tips and tricks.

2.4 Perceptual and actual behaviour of peers

The majority of previous research on the role of friends in delinquency has been based on perceptual, or indirect, measurements of friends' delinquency. These measurements entail asking respondents about their *perception* of their friends' delinquency levels. However, this means that one cannot be sure whether the *actual* delinquent behaviour of friends is related to individual offending, but only that people's perception of their friends' delinquency levels is related to this. Recent research suggests that respondents tend to overestimate the similarity between their friends' delinquent behaviour and their own levels of delinquency (Boman et al., 2016; Weerman & Smeenk, 2005). Therefore, perceptual measurements can be considered questionable. Unfortunately, this method lies at the base of most previous studies on the relationship between delinquent friends and individual offending.

More objective approximations of friends' delinquency can be calculated by combining social network questions with self-report data on delinquency. This means asking respondents to report only on their own levels of delinquency, as well as asking them who their friends are in the network – and these friends themselves are then also asked to provide self-reports on their delinquency levels. Research on traditional offending based on these more objective or direct measurements suggests that the relationship between friend delinquency and individual offending is considerably less strong than previously assumed (Kandel, 1996; Weerman & Smeenk, 2005).

2.5 Analysing both influence and selection: findings for traditional delinquency

The substantial reliance on perceptual measurements of peer influence is not the only shortcoming in previous research on peer delinquency. Another limitation is that most of these studies on peer delinquency do not directly examine selection effects as a potential explanation for the relationship between peer delinquency and individual offending.[1] The main reason for this is that, for a long time, no sophisticated methods existed to enable

[1] Longitudinal peer influence studies that try to address selection effects generally did so by including measures of previous individual offending in wave *t*-1 as a control variable for individual offending in wave *t* (Gallupe et al., 2018). Whereas these attempts suggested that influence effects were likely to be smaller than previously estimated, this method is considered to be inadequate for estimating true influence and selection effects (Haynie & Osgood, 2005).

researchers to analyse how individuals' behaviour and their social network structure mutually affect one another. Doing so requires a model in which longitudinal data on both the network structure and individual behavioural characteristics are analysed as joint dependent variables (Steglich et al., 2010). Recently, a new family of statistical models has been developed that enables researchers to do precisely this: stochastic actor-oriented models (SOAMs, also often referred to as SIENA models; see, for example, Ripley, Snijders, & Preciado, 2020; Snijders, 2001; Snijders et al., 2010; Steglich et al., 2010). Chapter 6 will elaborate on these models in more detail.

In recent years, a number of more sophisticated studies on selection and influence effects of peer delinquency have been published. Several of these studies found a positive and statistically significant influence effect of delinquent peer behaviour on traditional individual delinquency, while controlling for selection effects (see, for example, Baerveldt, Völker, & Van Rossem, 2008; Burk, Kerr, & Stattin, 2008; Burk et al., 2007; Jose, Hipp, Butts, Wang, & Lakon, 2016; Kerr, Van Zalk, & Stattin, 2012; Osgood, Feinberg, & Ragan, 2015; Snijders, Van de Bunt, & Steglich, 2010; Svensson, Burk, Stattin, & Kerr, 2012; Weerman, 2011). Similar findings have been published regarding other forms of antisocial behaviour in a broader sense (Logis, Rodkin, Gest, & Ahn, 2013; Molano, Jones, Brown, & Aber, 2013; Rulison, Gest, & Loken, 2013; Shin, 2017). A few studies did not find a significant influence effect of delinquency (Haynie, Doogan, & Soller, 2014; Knecht, Snijders, Baerveldt, Steglich, & Raub, 2010; Weerman, Wilcox, & Sullivan, 2018) or antisocial behaviour (Dijkstra, Berger, & Lindenberg, 2011). However, a recent meta-analysis that included all of the studies mentioned above reported an overall positive and statistically significant effect for influence, although the effect size can be considered small (Gallupe et al., 2018). Specifically, the meta-analysis found 'the odds of a person adjusting their level of offending to be one unit closer to that of their friends is 21% higher than not changing their level of offending' (*ibid.,* p. 323). The overall positive significant effect of the meta-analysis suggests that the *actual* level of friend delinquency influences individual delinquent behaviour.

Several studies also reported positive and statistically significant effects for peer selection on delinquency (Baerveldt et al., 2008; Burk et al., 2008, 2007; Haynie et al., 2014; Jose et al., 2016; Knecht et al., 2010; Osgood et al., 2015; Svensson et al., 2012) and antisocial behaviour (Kerr et al., 2012; Shin, 2017; Van Zalk & Van Zalk, 2015). However, several other studies found no statistically significant effect for selection on delinquency (De la Rue, 2015;

Molano et al., 2013; Snijders et al., 2010; Turanovic & Young, 2016; Weerman, 2011; Weerman et al., 2018) or antisocial behaviour (Dahl & Van Zalk, 2014; Dijkstra et al., 2011; Logis et al., 2013; Rulison et a.l, 2013). Here, the meta-analysis by Gallupe et al. (2018), too, found an overall positive effect for selection, albeit with a small effect size. Specifically, they found that 'A person has a 5% higher odds of forming a friendship tie with someone who has the same score on the offending scale than someone 1 unit less or more' (*ibid.*, p. 326).

In summary, the existing findings on selection and influence effects on traditional delinquency suggest that both processes play a small but significant role in individual offending behaviour.

2.6 Influence and selection in cyber-delinquency?

No previous research has been published analysing both influence and selection processes with regard to cyber-delinquency. A small number of studies have investigated the extent of any cross-sectional relationship between individual cyber-delinquency and that of friends, using perceptual measurements. The findings are uniform, with all these studies reporting a considerable positive relationship between individual cyber-offending and perceptions of friends' levels of cyber-delinquency (Bossler & Burruss, 2011; Holt et al., 2012, 2010; Marcum et al., 2014; Morris, 2011; Morris & Blackburn, 2009; Rogers, 2001; Skinner & Fream, 1997; Weulen Kranenbarg, et al., 2021).

Unfortunately, nearly all the previous studies on the relationship between individual cyber-offending and friends' levels of cyber-delinquency neglected traditional offending, thus making it hard to place the finding for cyber-offending in context. There are, however, indications that the relationship between individual offending and friends' offending is weaker for cyber-offending than for traditional offending. In their paper, Weulen Kranenbarg, Ruiter and Van Gelder (2021) made a direct comparison between cyber-offenders and traditional offenders and found that similarity in offending between individuals and their friends was weaker for cyber-offending than for traditional offending. One explanation for this finding is that it is relatively easy for online offenders to operate anonymously, and that online behaviour often has no offline consequences (Jaishankar, 2008; Suler, 2004). Additionally, many skills needed for conducting cybercrimes can be easily searched for online,

without the help of offline friends (Goldsmith & Brewer, 2015). All these aspects make it easier for individuals to hide their cyber-offending from their friends, leading to a situation in which friends (at least offline friends) play a smaller role than they would in traditional offending (Weulen Kranenbarg, et al., 2021).

In addition, as mentioned earlier in this chapter, existing studies on the role of peers in cyber-delinquency suffer considerable limitations. Firstly, no longitudinal research has yet been conducted on peer effects. This makes it unclear as to what extent similarity in cyber-deviance between peers is attributable to either influence or selection. Secondly, since all these studies relied on perceptual measurements for levels of friend delinquency, they can provide only an indication of the extent to which individual offending is influenced by the *perception* of the cyber-offending levels of an individual's friends. Finally, previous research scarcely studied the role of online friends in comparison to offline friends in cyber-delinquent behaviour. In nearly all previous studies, respondents were asked to report about the cyber-delinquent behaviour of their unspecified 'friends'. Hence, they were asked to report only on their friends in general, without having to distinguish between friends in the offline world, and online friendships that have evolved from communications on the internet. As mentioned in the introduction, this is problematic, given the multiple indications that contacts from online forums play an important role in the exchange of knowledge and opportunities for commiting cyber-offences (Holt, 2007; Hutchings, 2014). The few studies that did specifically distinguish between online and offline friend delinquency were limited to illegal downloading (Miller & Morris, 2016) or traditional delinquent behaviour (Meldrum & Clark, 2015), or did not distinguish between cyber-enabled and cyber-dependent crimes (Bunders & Weerman, 2020).

3. Research method

This research report focuses on cyber-delinquent behaviour of juveniles and young adults between 12 and (at most) 25 years of age, the period in which most delinquent behaviour occurs (Farrington, 1986; Sweeten, Piquero, & Steinberg, 2013). During this age period, the majority of people go to school or are in further education, where they form social networks with peers from their school class or other classes. Individuals often make extensive changes to their social network during this period, which makes the peer context dynamic (see, for example, Knecht et al., 2010). We therefore conducted a longitudinal survey at schools for secondary education (high schools, ages 12-17) and tertiary education (vocational schools, ages 16-25) in the Netherlands.

3.1 Recruitment of schools

In order to obtain a relevant sample for our study, we targeted schools that offered at least some type of Computer Science or ICT programme to their students. In this way, we aimed to include a relatively high number of respondents with ICT skills and who were thus at an increased risk of being involved in cyber-offences. This purposive sampling approach was necessary, as our analyses required a sufficient prevalence of and variability in cyber-offending among respondents.

Our sampling strategy was as follows. Using open source educational data,[2] we first selected secondary education institutions that offered some type of ICT classes to their students (age range in sample: 12-17; mean = 14.7 years). In the Dutch educational system (which differs from the UK school system), children who have finished primary school are assigned to a specific level of secondary education, based on their primary school grades. There are three levels: pre-vocational secondary education (the 'lowest' level), general secondary education (the 'middle' level) and pre-university education (the 'highest' level). In order to obtain a broad sample, we targeted all three types of secondary schools.

[2] See https://duo.nl/open_onderwijsdata/databestanden/vo/leerlingen/.

Schools for pre-vocational secondary education (known in the Netherlands as 'vmbo' schools) were eligible for inclusion in our sample only if at least 20 of their pupils had taken final examinations in ICT[3] in 2018 (the most recent year for which data were available during our study). Thirty-five vmbo schools across the Netherlands met this requirement. We approached the five vmbo schools with the highest number of ICT students. Of the remaining 30 vmbo schools, we randomly selected 15. For practical reasons we excluded two of these schools, as they were located more than two hours' travelling time from Amsterdam. In total, 18 vmbo schools were sent a letter inviting them to participate in our research.

Next, we approached schools that offered general secondary education (in Dutch: 'havo' schools) and/or pre-university education (in Dutch: 'vwo' schools). These schools were selected only if more than 40 pupils[4] (havo or vwo, or both combined) had taken their final examinations in Computer Science in 2018. We excluded schools that were more than two hours' travelling time from Amsterdam. Of the 93 schools that met these requirements, we selected the six[5] schools with the highest number of ICT students. From the next top 50 schools in the list, we randomly selected a further 25 havo and/or vwo schools.

We also invited tertiary educational institutions to participate in our research (age range in sample: 14-25; mean = 17.4 years). As in the secondary education system, there are also three broad tertiary education levels in the Netherlands. However, we only targeted vocational education schools (in Dutch 'mbo' schools), given that they are the only types of schools that require intensive attendance in classes of limited size.[6] Using open source data from the Dutch Ministry of Education, Culture and Science,[7] we selected mbo institutions that offered specific ICT programmes (ICT Management, and Application and Media Development)

[3] These ICT requirements were met if pupils were enrolled in the elective Media, Design and ICT profile (*onderwijsprofiel Media, Vormgeving en ICT*) or the ICT route (*ICT-route*), or if they had completed the subjects Media and ICT (*Vormgeving en ICT*), Application design (*Applicatieontwikkeling*), Digital security (*Digitale beveiliging*), Game design (*Game design*), ICT (*ICT/Informatietechnologie*), Computer Science (*Informatica*), or Media, Design and Network Management (*Media, Vormgeving en Netwerkbeheer*).

[4] We used a larger cut-off criterion for havo/vwo schools than for vmbo schools because the havo/vwo schools tended to have much higher numbers of ICT students than the vmbo schools.

[5] As two havo/vwo schools in the top five had the same number of ICT students, there were six schools in the havo/vwo schools top five of ICT students.

[6] The other two types of tertiary education (higher professional education/applied universities and academic institutions/universities; in Dutch: hbo and wo) mainly provide their education through large-scale lectures, and have very low attendance requirements. Conducting research at these institutions would not only have been very hard to organise, but, most importantly, it would not have resulted in complete cohorts of participating students – a requirement for the longitudinal study of friendship school networks.

[7] See https://www.kiesmbo.nl/.

and courses on Media, Design and Technology. Thirty-eight of these schools were located within two hours' travelling time from Amsterdam. We randomly selected 20 of them. Because four of these only offered adult education or self-study, or had very small ICT departments, 16 mbo institutions were sent an invitation.

Of all the schools that were sent an invitation, seven schools (one vmbo school and six mbo institutions) decided to participate in our research. Because we aimed for more schools in our sample, we decided to conduct an additional recruitment round, using more direct and innovative ways to approach schools. The main researcher of this report contacted eleven ICT teachers with an inviting and noticeable profile on LinkedIn. This resulted in five more schools deciding to participate in our study (one havo/vwo school, two vwo schools, and two mbo institutions).

Table 1: Respondent numbers and participation rates for each school in waves 1, 2 and 3

School number (type)	Number of respondents wave 1	Number of respondents wave 2	Number of respondents wave 3	Relative participation rate wave 1*	Number in wave 1 and 2 (% of wave 1)
School 1 (mbo)	91	81	0	B (60-80%)	75 (82.4%)
School 2 (havo/vwo)	92	88	24	B (60-80%)	77 (83.7%)
School 3 (vmbo)	62	75	13	C (25%)	59 (95.2%)
School 4 (mbo)	30	30	24	A (90-100%)	28 (93.3%)
School 5 (mbo)	47	46	28	A (90-100%)	42 (89.4%)
School 6 (vwo)	32	34	33	A (90-100%)	32 (100%)
School 7 (mbo)	39	30	12	B (60-80%)	29 (74.4%)
School 8 (mbo)	52	43	9	B (60-80%)	35 (67.3%)
School 9 (mbo)	56	58	9	A (90-100%)	53 (94.6%)
School 10 (vwo)	36	34	30	A (90-100%)	32 (88.9%)
School 11 (mbo)	129	99	23	C (25%)	87 (67.4%)
School 12 (mbo)	226	189	113	B (60-80%)	175 (77.4%)
Total	892	807	318	B (60-80%)	724 (81.2%)

vmbo = pre-vocational secondary education
havo = general secondary education
vwo = pre-university secondary education
mbo = tertiary vocational education
** Participation rates are estimates as schools could not provide us with a list of all the potential respondents.*

3.2 Participant recruitment

We recruited the students in collaboration with the participating schools. A few weeks before the start of the study, participating schools distributed digital information and consent forms, developed by the researchers, to their students. These forms stated that our research was aimed at gaining a better understanding of the cyber-behaviour, both legal and illegal, of students in the Netherlands. Students were also informed that the research would be conducted in their own classroom during normal school hours and supervised by independent researchers. In order to encourage participation, the forms also mentioned that a voucher for 20 euros per school would be raffled at the end of each wave.

In order to participate in the research, invited students had to register in advance. This was so that we could include them in the list of potential friends in the network. To comply with the European regulations on privacy, we also had to obtain permission from the parents of all the secondary school pupils and mbo students under the age of 16, in addition to obtaining their own consent. We therefore included a consent form for the parents in the material sent to these students.

3.3 Sample

The total sample of the study consisted of respondents from eight schools for tertiary education and four schools for secondary education. We collected data in three waves. Wave 1 was conducted between September and November 2019, with 892 respondents participating in this first round of data collection. Wave 2 was conducted in January and February 2020, with 807 respondents participating in this follow-up round. Wave 3 took place during the COVID-19 crisis, in June 2020, when schools were not fully operational. Despite the pandemic measures that were in place at the time, we nevertheless managed to conduct a survey, albeit with a smaller sample size – 318 respondents.

Participation rates varied between schools, mainly because of the different ways in which the educational institutions choose to distribute the participation forms (for detailed information about participation rates, see Table 1). In the case of three mbo institutions, the participation rate in wave 1 was between 90 and 100 per cent (n = 133); four mbo schools had a participation rate of between 60 and 80 per cent (n = 408), while at one mbo we reached

only 25 per cent of all eligible students (*n* = 129). Two secondary schools participated with a whole cohort of ICT and non-ICT pupils, with participation rates of 70 per cent and 25 per cent respectively (*n* = 154 for both schools together). Lastly, two secondary schools participated with two ICT classes each, with participation rates of around 95 per cent (total *n* = 68).

There were two main reasons why students did not participate in our study: a) they were unable to get the required parental permission in time, or b) they were reluctant or unwilling to take part. With respect to the second reason, researchers who were present during the data collection noticed that the willingness to participate seemed to work contagiously: once one student participated, the general tendency was for friends of this student to participate as well. This means that, despite the presence of sometimes substantial levels of non-response, the friendship networks researched will probably be relatively complete.

A total of 724 respondents who participated in wave 1 also completed the survey in wave 2. The total size of wave 2 was 807 respondents because of 83 new respondents ('births') in wave 2. Conversely, 167 respondents dropped out in wave 2 after having filled in the survey in wave 1. The reasons for non-participation in wave 2 were diverse. In some cases, students had switched study courses, or had dropped their ICT classes. Others were absent or ill on the second day of our study. Finally, some respondents decided to drop out of our study because they were no longer interested in participating.

3.4 Procedure

In waves 1 and 2, respondents completed a digital questionnaire on a computer in their own classroom during school hours. Classmates who had not registered to participate in our research worked on another assignment. At least one researcher was present when the questionnaire was administered in the classrooms. On average, respondents took 25 minutes to complete the survey in wave 1, and 21 minutes to complete it in wave 2.

Because of the COVID-19 measures that were in place in June 2020, wave 3 had to be organised differently. Since national policy required schools to teach through distance-learning, participating respondents completed the digital questionnaire from home instead of at school. Respondents took an average of 23 minutes to complete this survey. Because

we were unable to contact respondents directly in these circumstances, wave 3 suffered high dropout numbers. This also led to incomplete information on the school friend networks. Therefore, we were unable to use the school friend networks for wave 3. However, the data from waves 1 and 2 were sufficient for conducting our network analyses.

3.5 Operationalisation of delinquency and peer measures

For this study, we developed a questionnaire that included various multiple-item measures. A description of the central variables used in the analysis, and how these were measured, is provided below.

- Individual offending of respondents (waves 1, 2)

  We used the self-report method to get an indication of how many respondents were involved in various types of online delinquency (cyber-enabled and cyber-dependent) and traditional (offline) offending. Respondents were asked how often they had committed various cyber-dependent, cyber-enabled and traditional crimes in the previous three months. Table 2 provides an overview of all the individual items and their corresponding category of offences. Table 2 provides an overview of the wording of all the individual delinquency variables.

  The possible answer categories were '0 times' (0), '1 time' (1), '2 times' (2), '3-5 times' (3), '6-10 times' (4), 'more than 10 times' (5) and 'Don't know/Prefer not to say'. To arrive at a scale measure, answers to the separate individual delinquency questions were first dichotomised. If, for example, a respondent indicated that they had hacked one or more times, their hacking score was encoded as 1. If a respondent indicated no hacking in the previous three months, this score was encoded as 0. After dichotomisation, all the scores for each delinquency category (cyber-dependent, cyber-enabled, traditional) were added to create a measure of variation for each delinquency category that reflected the *number of different offences* committed. This variety measure is preferred over a frequency measure because the latter would overemphasise frequently reported minor offences (Sweeten, 2012; Weerman, Bijleveld, & Averdijk, 2005). Scores on these three delinquency variables were coded as missing *only* when a respondent had indicated 'Don't know/Prefer not to say' for all offences within an offence category.

Table 2: Overview of different delinquency categories and their respective items

	Offence type	Item: "How many times in the past three months did/were you (without permission)…"
CYBER-DEPENDENT	Hacking guess (1)	… hack by guessing, peeking or filling in someone's password yourself?
	Hacking technical applications (4)	… hack through technical applications that help you guess passwords automatically? For example, rainbow tables, brute force, or a key logger. … hack through exploits? These are programs or a piece of computer code that you can use to exploit vulnerabilities in software. … hack through SQL injections? An SQL injection enables you to read, modify or even delete databases. … hack in a way not mentioned in the previous questions about hacking?
	Stealing or destroying data (3)	… copy digital files or data belonging to someone else? … modify, delete, or add something to another person's digital files or data? ... alter the content of a web page, so that, for example, the website displayed a different message from what its owners intended? (web defacement)
	DDoS attacks (2)	… carry out a (D)DoS attack WITHOUT having set it up yourself? … carry out a (D)DoS attack that you had set up (or partly set up) yourself?
	Malware (2)	… deliberately spread or use some form of malware? ... design or develop (or partly design or develop) a form of malware?
CYBER-ENABLED	Editing video/audio files (1)	… edit video or audio material to make others feel angry/afraid/ashamed/unhappy?
	Online conflicts (2)	... involved in online quarrels or conflicts? For example, scolding or bullying someone online or trying to scare someone online. … in online conflicts about you disclosing sensitive information? E.g. nude photos.
	Online fraud (2)	… commit fraud on the internet? For example, posing as someone else online, using someone else's online data to make money, selling fake tickets online, selling something over the internet but never sending the product, or buying something over the internet but never paying for it. … use your bank account (or your parents') to transfer money? (money mule)
	Illegal trade (1)	… buy or sell illegal items on the internet (e.g. the dark web)? Examples are login details, bank details, identity details, drugs, weapons, etc.
	Phishing (1)	… try to obtain someone's login data through phishing (e.g. through a fake bank website or app) or try to persuade someone to transfer money (e.g. by trying to pretend you were someone's friend and had money troubles)
TRADI-TIONAL	General traditional offences (5)	… steal something (from a shop, person or school, etc.)? … deliberately damage or destroy something that wasn't yours? … intentionally wound someone else? … break in somewhere, for example to steal something? … sell drugs or medication offline, such as weed, ritalin, XTC or cocaine?

Following these procedures, *cyber-dependent offending* of the respondent (or 'ego' in the network analysis in Chapter 6) was constructed, using twelve questions about offences such as hacking, malware and DDoS attacks. C*yber-enabled offending* was constructed based on various items on offences such as online fraud, illegal trade and online conflicts (in wave 1, we used 17 detailed items to construct this variable, but these were grouped into seven items of a more general nature in wave 2 to reduce the burden

for the respondents). *Traditional offending* was calculated using five items on offences such as vandalism, burglary and violence.

- Friendship network (waves 1, 2)

  Respondents provided information about their friendship networks within their school cohort. All participants had access to a numbered list of names of all the respondents in their school who had registered beforehand. The text provided to respondents was as follows: 'We have provided you with a list of pupils or students from your school (cohort). Which pupils/students do you consider to be your friends? By "friends", we mean school mates that you like and whom you regularly hang out with. Please fill in the NUMBERS that are next to your school friends' names. You can decide for yourself how many people you select as your friend, up to a maximum of 10 people. You can also decide not to fill in a number, or only to fill in the numbers of one or two people.' In wave 1 respondents reported an average of 4.19 friends (range 0 – 10; *SD* = 3.05). In wave 2 they reported an average of 4.71 friends (range 0 – 10; *SD* = 3.36).

  The questions on friendship networks served to create the direct measures of actual self-reported friend delinquency for cross-sectional analyses of variables used in Chapter 5 (see below). They also served as input for the longitudinal network analyses in Chapter 6.

- Perceptual (indirect) measures of friend delinquency (wave 1)

  We measured respondents' perception of the offending behaviour of their friends by asking them how many of their friends had committed cyber-dependent, cyber-enabled or traditional offences? Respondents were asked to report on the delinquency levels of their school friends, their offline friends outside school (e.g. friends from the neighbourhood or sports club) and their online friends (i.e. friends that respondents spoke to only online, e.g. gaming friends). The time period to which these indirect questions about friends' offending referred was the same as for self-reporting, i.e. three months.

  Because we did not want to burden the respondents too much, we did not ask about their perception of their friends' involvement in all offences separately. Instead, all the offences were grouped together (see Table 2, again, for the groupings). An example of an item in the cyber-dependent category is 'How many of your school friends have set up, executed or ordered a DDoS attack in the past 3 months?' This was a grouping of the two

original DDoS options: conducting a DDoS attack that you have designed yourself, and having DDoS attacks carried out by others.

Respondents could indicate whether they believed that none of their friends (0), some of their friends (1), about half of their friends (2), more than half of their friends (3), or all or almost all of their friends (4) in this group had committed the offences in question. They could also fill in that they did not know whether their friends were involved, and whether the question did not apply to a certain group of friends (e.g. because they did not have any online friends). This resulted in nine variables: *cyber-dependent delinquency school friends (perceived), cyber-dependent delinquency offline friends (perceived), cyber-dependent delinquency online friends (perceived), cyber-enabled delinquency school friends (perceived), cyber-enabled delinquency offline friends (perceived), cyber-enabled delinquency online friends (perceived), traditional delinquency school friends (perceived), traditional delinquency offline friends (perceived)* and *traditional delinquency online friends (perceived).*

A high score for these variables meant that respondents assumed that relatively high numbers of their friends were involved in this category of delinquent behaviour. Scores were coded as missing if respondents (1) indicated at least once that they did not know whether their friends committed offences within this category, or that this did not apply; *and* (2) never indicated that their friends *had* committed this category of offences.[8]

- Actual self-reported (direct) measures of friend delinquency for cross-sectional analyses (wave 1)

  To compare the perceptions of respondents about their friends with the actual behaviour of friends (or, rather, the behaviour reported by the friends themselves), we also constructed direct measures for friend delinquency. For this measure we used the network questions about school friends. Because these school friends themselves had also answered questions about their own delinquency as a respondent, the network data

[8] This is a conservative scoring method. It means that a score was also encoded as missing if a respondent had indicated for one offence within a category that they did not know whether their friends were doing this, or that this did not apply, but had indicated for the rest of the offences within that category that their friends were *not* doing this. It is possible that respondents did not want to fill in that their friends had done something, and therefore chose 'Don't know' or 'Doesn't apply'. This conservative way of scoring means it is certain that a negative score ('My friends *have not* committed this offence type') applies to all the offences questioned within that category.

made it possible to calculate the extent to which each respondent had school friends who had reported delinquent behaviour themselves. The cyber-dependent, cyber-enabled and traditional delinquency scores of all respondents' school friends were summed in order to calculate the direct (actual self-reported) delinquency measure of school friends (this was in order to obtain a measure of variation comparable to the individual delinquency scores).[9] This resulted in the following variables: *cyber-dependent delinquency school friends (direct), cyber-enabled delinquency school friends (direct)* and *traditional delinquency scores school friends (direct)*. This measure served mainly to contrast perceptual measures of friend delinquency with direct self-report measures (see Chapter 5). A different process was used for the longitudinal analyses about selection and influence processes with regard to actual delinquency of friends (see Chapter 6).

- General control variables (wave 1)

  Respondents indicated their *gender*, *age* and *education type*.

- Personal characteristics (waves 1 and/or 2; see Appendix for items)

  We also asked respondents about other individual factors that could potentially play a role in cyber-offending. These factors are explored in Chapter 4.

  - *Low self-control* is a composite measure and was calculated using nine items on traits such as impulsivity, anger and risk-taking behaviour, adapted from Grasmick, Tittle, Bursik, & Arneklev (1993). A high score on this variable indicates a low level of self-control. Self-control has been studied extensively in relation to traditional offending.
  - *Social skills* is a composite measure and was based on four items from the social competence scale by Lemmens, Valkenburg and Peter (2011). In the items, respondents answered questions about topics such as how easy they found it to talk about their feelings or to make contact with strangers. A high score on this variable indicates good social skills.

[9] We chose to use the sum of the total friend delinquency and not the average delinquency scores. This is because averaged scores could provide a distorted view of friend delinquency. If someone indicated they had ten friends, two of whom reported a lot of delinquent behaviour, while the other eight did not, that person would still get a low score for friend delinquency. By contrast, a respondent selecting only one friend, who in turn reported some delinquent behaviour, would get a relatively high score for friend delinquency. In short, an averaged score for friend delinquency is also strongly affected by the number of friends that someone selects. We decided to take the sum of the friend delinquency because this would seem to be a better indication of the total exposure to delinquency within the peer group.

- *Computer addiction* is a composite measure and was constructed using six items based on the game addiction scale developed by Lemmens, Valkenburg and Gentile (2015), who based their scale on the criteria for addiction as listed in the DSM-IV. For our measure, we used items on preoccupation, toleration, persistence, escapism, deception and problems.
- *ICT knowledge* consists of the answer to one question asking respondents to indicate what they considered to be their level of ICT knowledge (Holt et al., 2012; Rogers, 2001; Weulen Kranenbarg, 2018). Answer categories ranged from 'I don't like using computers and I don't use them unless I absolutely have to' to 'I can use different programming languages and I am capable of detecting programming errors.'
- *Gaming, average day* indicates how much time a respondent spent gaming on an average weekday.
- *Positive cyber-behaviour* is a variety measure and based on nine items. The coding procedure of this variable followed the same logic as the delinquency variety measures, but, contrary to delinquency, this measure indicates the extent to which respondents used their ICT skills for prosocial cyber-behaviour. Examples of such behaviour include helping others with computer problems, sharing self-developed code or software with others and attending hackathons.

- Environmental factors (waves 1 or 2; see Appendix for items)

  We also gathered information about the environmental risk factors (in the family and school context) that could be correlated with cyber-offending. These are also explored in Chapter 4.

  - *Offline rules by parents* is a composite measure, based on a measure used in the Dutch SPAN study (see, for example, Bruinsma, Pauwels, Weerman, & Bernasco, 2015; Hoeben & Weerman, 2016; Janssen, Weerman, & Eichelsheim, 2017). It consists of four items relating to the extent to which respondents' parents/carers know how, where and with whom respondents are spending their time, and whether parents have set clear rules about what respondents are allowed to do in their spare time.
  - *Online rules by parents* is a composite measure and serves as the online equivalent of the item concerning offline rules set by parents. It consists of four items relating

to the extent to which respondents' parents/carers know how, where and with whom respondents are spending their time online, and whether parents have set clear rules about internet and computer use.

- *Home alone, average day* consists of one item and indicates how many hours, on an average weekday, respondents are at home alone without parents or carers present. Previous studies found a lack of parental supervision to be related to higher levels of offending (Flanagan, Auty, & Farrington, 2019).
- *Computer alone, average day* consists of one item and indicates how many hours, on an average weekday, respondents spent on the computer without parents, carers or other authority figures knowing what they were doing.
- *Offline rules by school* is a composite measure and consists of four items on school rule clarity and school rule reinforcement (inspired by the work of Gordon, 2018; Nagin, 2013; Zullig, Koopman, Patton, & Ubbes, 2010).
- *Online rules by school* is a composite measure and consists of four items. It serves as the online equivalent of the offline rules by school.
- *School satisfaction* is a composite measure and consists of four items on the extent to which respondents were happy with and felt at home in their school (based on the NSCR School Study; see, for example, Weerman, 2010; Weerman & Hoeve, 2012), and whether they felt close to fellow students and teachers (see, for example, Haynie, 2002).
- *School boredom* consists of the answer to one question that asked respondents about the extent to which they felt school is boring (adapted from the NSCR School Study; see, for example, Weerman, 2010; Weerman & Hoeve, 2012).
- *ICT education satisfaction* is a composite measure that consists of two items on whether students felt they were being challenged during the ICT classes at school, and the extent to which they felt that they had learned new ICT skills at school.
- *Talk computer activities teachers* consists of the question of whether respondents talked about their computer activities with teachers.

Descriptive statistics for the individual and environmental variables can be found in Table 7 in Chapter 4. A codebook for these selected variables and the options for answering them can be found in the Appendix. A more extensive codebook, containing all the questionnaire's

original items in Dutch, together with their English translations, can be requested from the corresponding author.

3.6 General analytical strategy

Various analytical strategies were used to answer our research questions. A brief explanation is presented here. Each chapter describes the analytical method used in further detail.

Chapter 4 focuses on the role of general individual and environmental characteristics in cyber-delinquency. Using *negative binomial regression models* we aimed to determine which factors are correlates of cyber-offending, independently of the other factors. These type of regression models are specifically suited for analysing count data such as delinquency variety measures with a skewed distribution (i.e. with most scores at zero or close to zero).

Chapter 5 focuses specifically on the role of friends in cyber-offending. By collecting data on respondents' peer networks, individual offending and perceptions of friends' levels of delinquency, we were able to compare the respective relationships with offline and online friends to individual levels of cyber-offending. In addition, we compared correlations with individual levels of cyber-offending for actual and perceived cyber-delinquent behaviour of peers. For both analyses in this chapter, *Kendall's tau-b correlations* were calculated.

Chapter 6 zooms in further on the role of peers in cyber-offending. By using two waves of data on peer networks and cyber-offending behaviour and estimating *stochastic actor-oriented models*, we were able to study cyber-delinquency in relation to friendship network formation processes. Because these models can study friendship formation and behavioural changes over time, we were able to investigate the extent to which selection and influence effects play a role in cyber-delinquency.

3.7 Expert meeting

In October 2020 we organised an expert meeting with thirteen experts. Because of the COVID-19 pandemic, this meeting was held online on Zoom. Two different groups of experts were invited to this meeting. The first group consisted of three ICT teachers and one language tutor from the schools participating in the data collection. These experts informed us how cyber-delinquent behaviour was currently being handled in their schools and discussed how our results could help to improve prevention strategies among this target group. The second

group of nine experts was more diverse, but everyone in this group was involved in dealing with young cyber-offenders or in developing prevention measures for cybercrime among young people. They worked for various organisations: the police (two experts), Halt (an organisation for diversion, offering young first-time offenders a measure or small sanction to prevent future offending; one expert), a municipality (two experts), the Ministry of Justice and Security (two experts), the Dutch Platform for the Information Society (one expert) and the Child Protection Board (one expert).

The expert meeting lasted for two hours. In the first hour we presented our findings on individual characteristics of young cyber-offenders and asked experts to discuss these findings in two smaller groups (in breakout rooms). They discussed the extent to which they recognised the results in their daily work, how our results could be used in practice, and which future studies should follow up on this research. Afterwards we had a group discussion in which the experts reported their main conclusions. In the second hour we repeated this procedure for the environmental factors and the results for peer delinquency. The insights from the expert meeting are incorporated into the conclusions and implications discussed in the final chapter.

4. Results: cyber-delinquent behaviour and its risk factors

4.1 Introduction

This chapter focuses on our findings about the relationship between individual characteristics and environmental risk factors and cyber-dependent, cyber-enabled and traditional offending. We first provide an overview of the prevalence of each individual self-reported delinquent activity in our sample and then report how many respondents committed offences within each of the three main delinquency categories. We also describe how many respondents specialised in one offence category and how many had committed offences in more than one category. We then present descriptive statistics for potential individual and environmental correlates of cyber-offending. Next, we elaborate on the more advanced analyses (negative binomial regression) that we conducted to estimate the extent to which the investigated factors contribute to explaining individual levels of offending. We explain this technique and present the results of various models that were run for the three categories of offences. The chapter ends by providing answers to our first and fourth research questions: 'How are different types of cyber-delinquent behaviour among young people related to major individual characteristics and environmental factors?' and 'To what extent do these results differ between cyber-dependent, cyber-enabled and traditional delinquent behaviour?'

4.2 Delinquency variables

Table 3 provides an overview of the prevalence of the three different delinquency categories: cyber-dependent, cyber-enabled and traditional offending. It shows that a substantial proportion of the respondents had committed at least one offence within each category. Around half of the respondents reported at least one cyber-dependent offence in waves 1 and 2. For cyber-enabled offending and traditional offending, the number of respondents that reported having committed at least one offence was somewhat lower: 35 and 26 per cent, respectively, in wave 1, and 39 and 26 per cent in wave 2.

Table 3: Number of respondents who committed at least one offence in each category

	At least one offence, wave 1 (Total number of respondents = 892)		At least one offence, wave 2 (Total number of respondents = 807)	
	Number of respondents	(%)	Number of respondents	(%)
Cyber-dependent offending	456	(51.1)	366	(45.4)
Cyber-enabled offending	311	(34.9)	312	(38.7)
Traditional offending	232	(26.0)	207	(25.7)

Table 4 provides information about how often respondents had committed only one type of offence or combined offences from different categories.

Table 4: Combinations of offence categories

	Wave 1 (Total number of respondents* = 873)		Wave 2 (Total number of respondents* = 777)	
	Number of respondents	(%)	Number of respondents	(%)
No offending in any category	314	(36.0)	294	(37.8)
Only cyber-dependent offending	152	(17.4)	113	(14.5)
Only cyber-enabled offending	49	(5.6)	58	(7.5)
Only traditional offending	41	(4.7)	31	(4.0)
Cyber-dependent & cyber-enabled offending	126	(14.4)	110	(14.2)
Cyber-dependent & traditional offending	56	(6.4)	34	(4.4)
Cyber-enabled & traditional offending	24	(2.8)	30	(3.9)
All three categories	111	(12.7)	107	(13.8)

** The total number of respondents with no missing values in all three categories of offending. These numbers are therefore slightly lower than the numbers in Table 3.*

The table shows that a majority of offenders combined offences from at least two categories. Each wave, however, included a substantial portion of respondents who only committed cyber-dependent offences and no cyber-enabled or traditional offences. For cyber-enabled

and traditional offences, the percentage of respondents not committing any other offences is lower. However, the proportion of respondents who combined cyber-dependent or cyber-enabled offences with traditional offences was lower, and in fact the majority of cyber-offenders in both categories (around 58% in both waves) had not also committed traditional offencesc. Hence, while a minority specialised in only one category of offending, a majority specialised in cyber-enabled and/or cyber-dependent offences, with the most pronounced specialisation among cyber-dependent offenders.

Table 5 provides an overview of the prevalence of the specific offences within these different categories: the number and proportion of respondents in waves 1 and 2 who indicated that they had committed a delinquent activity in the three months prior to the questionnaire. We asked respondents about twelve separate cyber-dependent offences, seven separate cyber-enabled offences, and five separate traditional offences.

The most prevalent cyber-dependent offences, as shown in Table 5, were: (1) hacking through guessing passwords (reported by approximately a quarter of the respondents), (2) copying and vandalising data (i.e. copying digital files or data belonging to someone else and modifying, deleting or adding something to another person's digital files or data), which was reported by approximately one fifth of the respondents, and (3) hacking by using more technical means, which was still reported by over one in ten respondents. The offences least often reported were: (4) doing DDoS attacks, and (5) malware-related offences (in both waves, approximately five per cent of the respondents indicated that they had committed such an act).

With regard to cyber-enabled offending, offending rates were also found to vary between the different delinquent activities. The more interpersonal delinquency types were reported relatively often, in particular the category of online conflicts, which was reported by more than 30 per cent of the respondents in wave 2. Apart from online fraud (the second-highest self-reported offence), the other financial or property-related types of cyber-enabled delinquency were reported less often.

Table 5: Prevalence of offences in waves 1 and 2

	Separate offences per offence type	Number of respondents (%) who committed offences - wave 1 (total number of respondents in wave 1 = 892)		Number of respondents (%) who committed offence - wave 2 (total number of respondents in wave 2 = 808)[10]	
CYBER-DEPENDENT	Hacking: guessing	221	(24.8)	191	(23.6)
	Hacking: technical applications	103	(11.5)	88	(10.9)
	Hacking: exploits	143	(16.0)	93	(11.5)
	Hacking: SQL injections	78	(8.7)	61	(7.5)
	Hacking: other means	123	(13.8)	90	(11.1)
	Illegally copying files or data	202	(22.6)	180	(22.3)
	Vandalising or modifying data	162	(18.7)	133	(16.5)
	Defacing websites	89	(10.0)	71	(8.8)
	DDoS with help of others	47	(5.3)	47	(5.8)
	DDoS self	56	(6.3)	51	(6.3)
	Using malware	47	(5.3)	38	(4.7)
	Writing malware	39	(4.4)	42	(5.2)
CYBER-ENABLED	Editing video/audio files	96	(10.8)	75	(9.3)
	Online conflicts	200	(22.4)	263	(32.5)
	Online extortion	52	(5.8)	94	(11.6)
	Online fraud	135	(15.1)	50	(6.2)
	Money mule	14	(1.6)	22	(2.7)
	Illegal trade	42	(4.7)	39	(4.8)
	Phishing	47	(5.3)	29	(3.6)
TRADI-TIONAL	Stealing	138	(15.5)	110	(13.6)
	Vandalism	96	(10.8)	99	(12.3)
	Violence	87	(9.8)	79	(9.8)
	Burglary	11	(1.2)	16	(2.0)
	Offline drug selling/buying	46	(5.2)	53	(6.6)

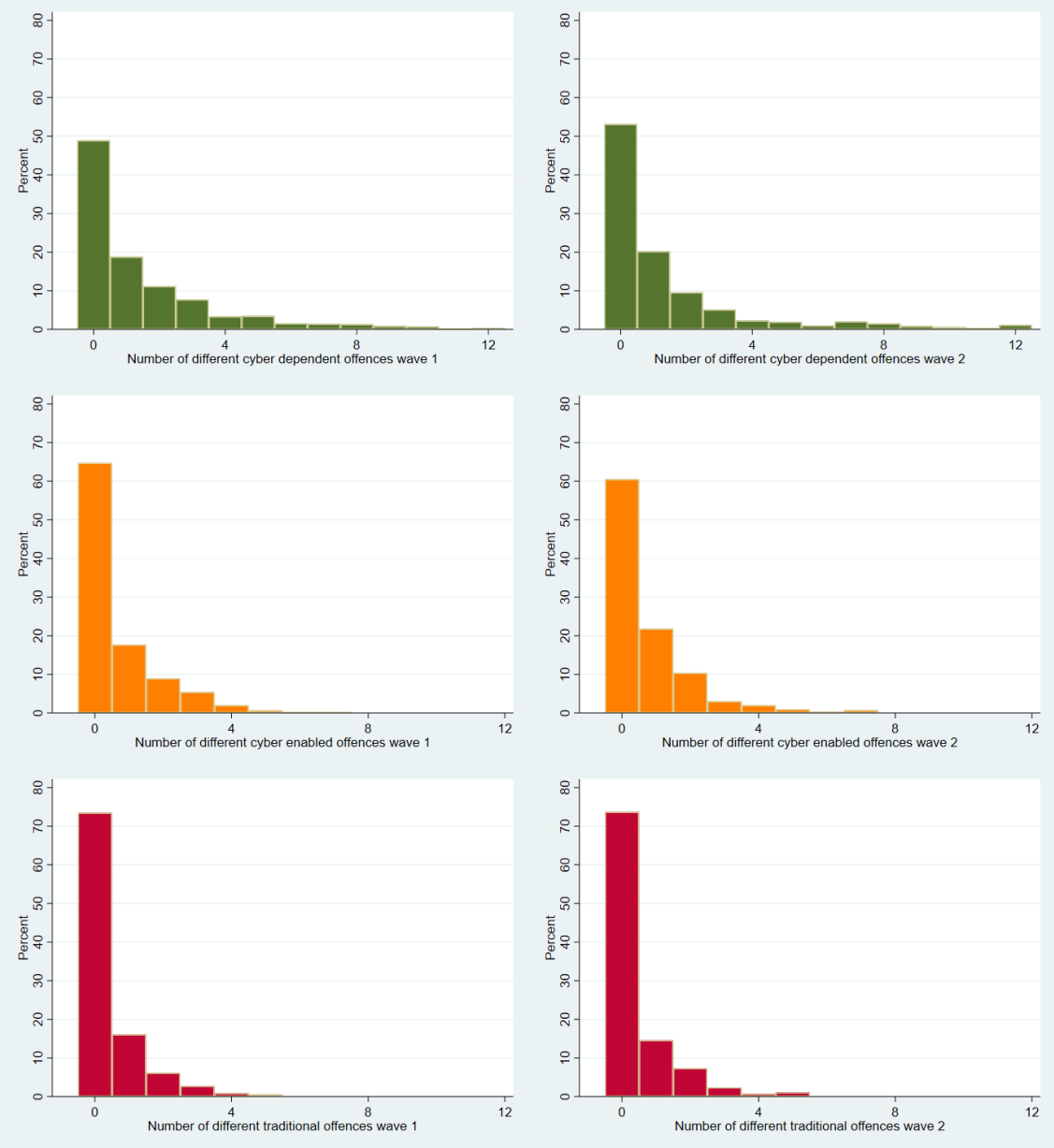
Differences in prevalence were also found to exist between the different offences within the traditional delinquency category. Here, stealing was reported most often (approximately 15 per cent in both waves), followed by vandalism (approximately 12 per cent); whereas burglary was reported by only a very small number of respondents (between 1 and 2 per cent).

Figure 1 presents an overview of the number of different offences committed by respondents for each offence category in each wave. This provides a better understanding of the distribution of offences committed across the sample. The histograms in Figure 1 show that, for each group of offences, most respondents indicated that they had committed no

[10] It is common for longitudinal studies to have smaller numbers of participants in subsequent waves than in the first wave.

offences. However, the histograms also demonstrate that a substantial number of respondents had committed one or more different offences. For instance, almost 20 per cent of the respondents had committed one cyber-dependent offence in waves 1 and 2, around 10 per cent two, and in total around 15-20% more than two.

Figure 1: Distribution of number of different offences for each category



In order to arrive at useable indices for total cyber-dependent, cyber-enabled and traditional offending for our further analyses, we created variety measures by summing the dichotomised delinquency scores for each subtype of offending. The score on these variables

indicates, for each respondent, how many *different offence types* that respondent reported to have committed in the three months prior to the questionnaire (see Chapter 3 for a detailed elaboration on this variable construction). Table 6 shows descriptive statistics for these indices.

Table 6: Descriptive statistics of the delinquency indices

Variable	Number of respondents	Mean	Standard deviation	Min.	Max.	Normalised mean*
OFFENDING BEHAVIOUR						
Cyber-dependent offending wave 1	892	1.47	2.20	0	12	.12
Cyber-dependent offending wave 2	781	1.39	2.41	0	12	.12
Cyber-enabled offending wave 1	882	0.66	1.13	0	7	.09
Cyber-enabled offending wave 2	788	0.73	1.23	0	7	.10
Traditional offending wave 1	875	0.43	0.87	0	5	.09
Traditional offending wave 2	787	0.45	0.92	0	5	.09

** The normalised mean has a range of 0–1 and is constructed by dividing the mean by the maximum value for the variable. As each category includes a different number of offences, this normalised mean is more suitable for comparing between the categories.*

Table 6 shows that, in both waves, the mean variety was the highest for cyber dependent offending in comparison to the other types of delinquency. This means that respondents committed, on average, relatively more cyber-dependent offence types than other offence types. This difference is visible when comparing the means as well as the normalised means (corrected for number of offence types within each category).

A comparison between the means of each category between the two waves reveals that, on average, there was no obvious increase or decrease in the number of offence types committed. However, this does not mean that there were no individual respondents who changed their level of delinquency, as will become clear in Chapter 6.

4.3 Individual characteristics and environmental risk factors

Having explored the prevalence of offending, we now turn to the individual characteristics and environmental factors that may have a relationship with cyber-dependent, cyber-enabled and traditional offending. It should be noted that the sample size and survey length did not

allow all potential risk factors to be included. The current study chose, therefore, to focus on some major individual and environmental factors identified in the literature. As many of these independent risk variables were only measured in wave 2, we decided to base the following analyses on the data from wave 2. Table 7 presents descriptive statistics for all the independent variables included (see Chapter 3 for an elaboration of the meaning and interpretation of these variables).

Table 7: Descriptive statistics of the individual and environmental variables

Variable	Number of respondents [11]	Mean	Standard deviation	Min.	Max.
INDIVIDUAL FACTORS (WAVE 2)					
Gender (female=1)	938	0.26	0.44	0	1
Age	949	16.71	1.99	12	25
Low self-control	804	2.92	0.66	1	4.89
Social skills	801	3.05	0.96	1	5
Computer addiction	904	1.38	0.40	1	3
ICT knowledge	907	2.27	0.86	0	4
Gaming, average day	793	1.07	1.30	0	5
Positive cyber-behaviour	798	2.67	2.13	0	9
ENVIRONMENTAL FACTORS (WAVE 2)					
Offline rules by parents	904	3.88	0.88	1	5
Online rules by parents	904	2.65	1.10	1	5
Home alone, average day	774	1.31	1.37	0	5
Computer alone, average day	757	1.39	1.51	0	5
Offline rules by school	805	3.66	0.85	1	5
Online rules by school	782	2.92	1.02	1	5
School satisfaction	810	4.15	0.72	1	5
School boredom	807	2.86	1.18	1	5
ICT education satisfaction	682	4.10	0.91	1	5
Talk computer activities teachers	781	1.80	1.08	1	5

Table 6 shows that the majority of our sample consisted of males: only 26 per cent of our sample was female. This is not surprising, given that ICT tends not to be a popular subject

[11] Participation numbers for wave 1 were 892 and 807 for wave 2. Note, however, that the *n* for some individual factors in this table exceeded 892. This is because we measured certain variables (e.g. gender and age) in both wave 1 and wave 2. Because of 'births' in wave 2, the number may exceed 892 participants.

among women in the Netherlands. In three of the eight tertiary education institutions in our sample, no females at all participated in our study. Most of the female participants in our study were in secondary education.

Substantial variation among the respondents was found in the values for the individual and environmental variables. However, it should be noted that school satisfaction in our sample was very high for most respondents (mean: 4.1 out of 5; *SD* = 0.7). Only a small number of respondents had a low score for this variable.

4.4 Analytical strategy for the regression models

Analysing self-reported delinquency data always entails the problem that offending behaviour is generally not normally distributed across the sample. This is also true for the current study: a substantial number of respondents reported no offending behaviour, and the distribution of responses among the others scores is highly skewed. Furthermore, our dependent variable is a count variable, and negative values are not possible. Using ordinary least squares (OLS) regression for such a variable is inappropriate (Field, 2013).

Instead we estimated negative binomial regression models. This is a type of regression analysis that belongs to the family of Poisson models; these are especially suited for count data because they do not predict negative values. Because our data are fundamentally skewed to the right and overdispersed (i.e. the variance is greater than the mean), we used negative binomial regression models.

For each category of offences, we ran three models: one for the individual characteristics only, one for the environmental factors only, and one for all factors. All negative binomial regressions were conducted in STATA 14.2 with the *nbreg*[12] command. The *fitstat* command was used in order to retrieve additional information on model diagnostics.

Tables 8, 9 and 10 (see below) report the *b* coefficient and standard error per variable. We also report the incidence rate ratios for each variable, which were obtained by exponentiating the coefficient. Such exponentiated coefficients are more insightful to

[12] Note that our observations were nested in schools. We therefore also ran multilevel negative binomial regressions with the *menbreg* command in Stata. The results did not differ from the results retrieved with the *nbreg* command. We therefore decided to report the results from our *nbreg* tests as this model provides more insightful information diagnostics than the *menbreg* models.

interpret because they show the expected change in the number of different delinquent acts committed (i.e. the dependent variable) if the independent variable were to increase by one.

Test statistics indicative of the goodness of fit were also included in our models. We reported the likelihood-ratio significance test results in order to show whether a model has a better fit than intercept-only models. McFadden's adjusted R^2 – which penalises a model if too many non-explanatory variables are included – is also reported in order to provide an additional measure for comparing the models' fit. McFadden's values are generally lower than normal R^2 values. Values between 0.2 and 0.4 are seen as an 'excellent fit' for a model (McFadden, 1977; UCLA, 2011). All three models that include only individual factors have McFadden's values around 0.1, which is acceptable. The models that include only environmental variables do not have a good fit, especially in the case of cyber-dependent offending, because McFadden's values for these models are low. The model fit for the final models, including both individual and environmental variables, improves for cyber-enabled and traditional offending, but not for cyber-dependent offending. This indicates that the environmental factors included here do not substantially add to the explanation of cyber-dependent offending. For all types of offending, the final model fit is acceptable and around 0.1.

Finally, we also conducted a robustness check to see whether the results of the regression models were driven mainly by the most prevalent but relatively minor offences of password guessing (for cyber-dependent offences) and having online conflicts (for cyber-enabled offending). These two offences may have biased our results, particularly if these minor offences were the only offences that respondents committed within a particular category. Our data indicated that 66 of the 191 respondents (32.5%, and so a substantial minority) who self-reported password guessing did not self-report any other cyber-dependent crime. Of the 263 respondents who self-reported online conflicts, 132 (50.2%, or more than half of this group of respondents) did not self-report any other cyber-enabled crime. Our robustness checks indicated that the results changed only marginally if these respondents were left out of the analyses: a few effects that were on the border of significance changed from significant to non-significant, or vice versa. These differences are noted in footnotes in the results section below.

4.5 Exploring the relationship between individual characteristics, environmental factors and offending

Tables 8, 9 and 10 present the results of our negative binomial analyses for the different types of delinquency. In the subsequent pages we discuss these tables together by describing the similarities and differences in effects between the tables. To ease interpretation, we highlighted the factors that were statistically significant. Green numbers represent a statistically significant positive relationship, while red numbers represent a statistically significant negative relationship. As mentioned earlier, the incidence rate ratio (IRR) is most informative because it represents the expected change in the dependent variable for a one unit increase in the predictor variable, assuming the other variables are held constant. For instance, the third model in Table 8 shows that if a respondent were to increase his level of computer addiction by one point while all other variables in the model are held constant, his number of different cyber-delinquent acts would be expected to increase by a factor of 1.381.

The first part of the following tables present the results for the demographics (gender and age) and the individual characteristics, not controlled of environmental factors. This provides an estimation on how strong the individual variables are related to one of the offence categories, independently from each other. The second part of the three tables present results for the environmental factors, but only controlled for the basic demographics but not for the individual characteristics. The third part of the table shows the results of the final models, in which each estimate is controlled for the other effects in the regression models for the individual as well as environmental variables. In else, this show us the most complete picture of how strongly each variable is related to an offence category, independent from the other variables.

Table 8: Negative binomial regression results for the effects of individual characteristics and environmental factors on cyber-dependent offending[13]

	Individual only (Number of respondents included in analyses = 691)			Environmental only (Number of respondents included in analyses = 524)			Individual + environmental (Number of respondents included in analyses = 521)		
INDIVIDUAL FACTORS	*b*	SE	IRR	*b*	SE	IRR	*B*	SE	IRR
Gender	-0.382*	0.164	0.683	-0.619**	0.208	0.538	-0.284	0.197	0.752
Age	-0.035	.027	0.966	-0.090*	0.038	0.914	-.103**	0.034	0.902
Low self-control	0.422***	0.086	1.526				0.393***	0.102	1.482
Social skills	0.274***	0.058	1.315				0.297***	0.066	1.346
Computer addiction	0.374*	0.152	1.453				0.323*	0.160	1.381
ICT knowledge	0.080	0.070	1.083				0.164*	0.079	1.178
Gaming, average day	0.067	0.043	1.069				0.084^	0.048	1.088
Positive cyber-behaviour	0.296***	0.026	1.344				0.266***	0.029	1.304
ENVIRONMENTAL FACTORS									
Offline rules by parents				-0.036	0.099	0.963	-0.100	0.088	0.905
Online rules by parents				-0.093	0.077	0.912	-0.047	0.067	0.954
Home alone				0.140*	0.055	1.150	0.044	0.047	1.044
Computer alone				0.126*	0.050	1.135	-0.012	0.045	0.988
Offline rules by school				0.001	0.100	1.000	-0.074	0.086	0.928
Online rules by school				0.026	0.083	1.026	-0.003	0.073	0.997
School satisfaction				0.143	0.114	1.154	-0.055	0.102	0.946
School boredom				0.103	0.065	1.108	-0.048	0.059	0.953
ICT education satisfaction				-0.062	0.085	0.940	0.087	0.073	1.091
Talk computer activities				0.208***	.064	1.231	-0.008	0.059	0.992
Constant	-3.083***	0.631	0.046	0.775	.987		-1.240	0.965	0.289
Log likelihood	-940.409			-826.522			-750.56		
McFadden adj. R2	0.115			0.014			0.093		

Symbols for significance: *** = *p* <.001; ** = *p* <.01; * = *p* <.05; ^ = *p* <.10; red = statistically significant negative effect; green = statistically significant positive effect.

[13] Excluding password guessing from the dependent variable in the models in Table 8 showed the results to be robust when this is excluded. The only difference found between these models was that gaming changed from marginally significant in model 3 (p =.08) for cyber-dependent offending including password guessing to non-significant (p =.10) in model 3 excluding password guessing. As this result was already only marginally significant, this is still a very minor change in results. It shows that the results of gaming are not very strong.

Table 9: Negative binomial regression results for the effects of individual characteristics and environmental factors on cyber-enabled offending (N = 694 - 525)[14]

	Individual only (Number of respondents included in analyses = 694)			Environmental only (Number of respondents included in analyses = 525)			Individual + environmental (Number of respondents included in analyses = 522)		
INDIVIDUAL FACTORS	*b*	SE	IRR	*b*	SE	IRR	*b*	SE	IRR
Gender	-0.193	0.162	0.824	-0.145	0.190	0.865	-0.002	0.185	0.997
Age	-0.099***	0.030	0.906	-0.173***	0.039	0.840	-0.150***	0.035	0.860
Low self-control	0.449***	0.088	1.566				0.453***	0.098	1.572
Social skills	0.199***	0.059	1.220				0.214***	0.065	1.239
Computer addiction	0.574***	0.141	1.776				0.567***	0.141	1.763
ICT knowledge	-0.160*	0.074	0.852				-0.093	0.078	0.911
Gaming, average day	0.060	0.044	1.062				0.047	0.048	1.048
Positive cyber-behaviour	0.201***	0.026	1.224				0.180***	0.028	1.198
ENVIRONMENTAL FACTORS									
Offline rules by parents				-0.055	0.093	0.946	-0.037	0.084	0.963
Online rules by parents				-0.150*	0.077	0.860	-0.133^	0.071	0.876
Home alone				0.181***	0.050	1.192	0.089*	0.045	1.093
Computer alone				0.107*	0.045	1.113	-0.033	0.044	0.967
Offline rules by school				0.006	0.096	1.006	-0.100	0.085	0.904
Online rules by school				-0.043	0.082	0.958	-0.076	0.073	0.926
School satisfaction				-0.149	0.106	0.862	-0.233*	0.097	0.792
School boredom				0.125*	0.064	1.132	-0.017	0.058	0.983
ICT education satisfaction				0.125	0.082	1.134	0.171*	0.076	1.187
Talk computer activities				0.229***	0.063	1.257	0.077	0.057	1.078
Constant	-1.877**	0.652	0.153	2.159*	0.958	8.661	0.004	0.942	1.004
Log likelihood	-713.302			-608.576			-556.331		
McFadden adj. R2	0.093			0.030			0.098		

Symbols for significance: *** = p <.001; ** = p <.01; * = p <.05; ^ = p <.10; red = statistically significant negative effect; green = statistically significant positive effect

[14] Excluding online conflicts from the dependent variable in Table 3 showed that this results in only minor changes in the environmental factors. In both model 2 and model 3, the effect of online rules by parents decreased to non-significant (from p =.05 to p =.11 in model 2, and p =.06 to p =.21 in model 3). As this effect was already only marginally significant in the final model including online conflicts, this shows that this result is not very strong.

While the effect of online rules by parents disappears if online conflicts are excluded, a new effect of online rules by schools appears in the final model. It seems that parents have slightly more influence on online conflicts, while schools have slightly more influence on the other cyber-enabled crimes.

While the effect of talking about computer activities changed to not significant in the final model including online conflicts (p =.18), it is still marginally significant in the final model excluding online conflicts (p =.06).

Table 10: Negative binomial regression results for the effects of individual characteristics and environmental factors on traditional offending (N = 693 - 521)

	Individual only (Number of respondents included in analyses = 693)			Environmental only (Number of respondents included in analyses = 524)			Individual + environmental (Number of respondents included in analyses = 521)		
INDIVIDUAL FACTORS	*b*	SE	IRR	*b*	SE	IRR	*b*	SE	IRR
Gender	-0.468*	0.206	0.626	-0.087	0.244	0.916	-0.044	0.241	0.956
Age	-0.177***	0.045	0.837	-0.230***	0.054	0.794	-0.186***	0.051	0.830
Low self-control	0.942***	0.120	2.565				0.796***	0.135	2.216
Social skills	0.211**	0.079	1.236				0.278**	0.090	1.320
Computer addiction	0.465*	0.192	1.593				0.569*	0.196	1.767
ICT knowledge	-0.309**	0.104	0.734				-0.244*	0.109	0.783
Gaming, average day	-0.041	0.063	0.959				-0.051	0.068	0.949
Positive cyber-behaviour	0.120***	0.036	1.128				0.168***	0.040	1.184
ENVIRONMENTAL FACTORS									
Offline rules by parents				-0.351**	0.122	0.704	-0.296**	0.114	0.744
Online rules by parents				-0.039	0.102	0.962	-0.016	0.099	0.984
Home alone				0.118^	0.068	1.125	0.034	0.065	1.035
Computer alone				0.039	0.062	1.040	-0.114^	0.063	0.892
Offline rules by school				0.308*	0.128	1.362	0.177	0.118	1.193
Online rules by school				-0.143	0.106	0.866	-0.210*	0.099	0.810
School satisfaction				-0.356*	0.140	0.700	-0.422**	0.136	0.655
School boredom				0.238**	0.085	1.270	0.082	0.079	1.086
ICT education satisfaction				0.367***	0.113	1.444	0.425***	0.112	1.529
Talk computer activities				0.192*	0.082	1.212	0.021	0.081	1.022
Constant	-1.74	0.913	0.175	2.335^	1.296	10.329	-0.932	0.322	0.394
Log likelihood	-533.403			-445.666			-404.675		
McFadden adj. R2	0.091			0.046			0.114		

Symbols for significance: *** = p <.001; ** = p <.01; * = p <.05; ^ = p <.10; red = statistically significant negative effect; green = statistically significant positive effect.

4.5.1 Results for individual factors

With regard to *gender*, the first models in the tables on individual characteristics show that males reported a greater variety of cyber-dependent and traditional offences than females. However, when controlled for environmental factors in the final model, these gender effects disappear. This means that these environmental factors can (at least partly) explain the differences between males and females. Therefore, results in the final models show us the

most complete picture: gender does not seem to add much to the explanation of differences in offending in our sample.

With regard to *age*, we found that younger respondents tended to report a greater variety of cyber-enabled and traditional offences than older respondents, also in the final model. For cyber-dependent offences, no effect of age was shown in the first model, but the final model also showed that younger respondents tended to report a greater variety of cyber-enabled and traditional offences than older respondents when controlled for environmental factors.

Low self-control is related to all types of delinquent behaviour: the lower someone's self-control, the higher the offending variety score across all models. Although some previous (but not all) studies found that high self-control was related to more cyber-dependent offending (see, for example, Van der Wagen, Van 't Zand-Kurtovic, Matthijsse, & Fischer, 2019), this was not found to be the case in our study. However, the incidence rate ratios in the final model suggest that the effect is more pronounced for traditional offending (IRR=2.2) than for cyber-enabled offending (IRR=1.6) and cyber-dependent offending (IRR=1.5).

Surprisingly, *social skills* were positively related to all types of delinquency across the models. In other words, respondents who reported a higher score on social skills (operationalised in this study as the ability to make friends and talk about your feelings easily) also tended to report higher levels of offending. While the level of statistical significance varied between the different types of delinquency, the incidence rate ratios were similar.

Computer addiction was related to all three types of offending across all models. This means that computer addiction might be a risk factor for delinquent behaviour in general. In contrast to what might be expected, however, the incidence rate ratios suggest that computer addiction was not more strongly associated with cyber-dependent offending than with the other two types of offending.

We found a small but positive effect of *ICT knowledge* for cyber-dependent offending, but only in the final model. In addition, ICT knowledge seems to be negatively related to traditional offending. For cyber-enabled offending, a small negative effect was found in the first model, but this disappeared in the final model. It should be noted that, in contrast to previous research, many students in our sample of ICT schools may have the skills to commit cyber-dependent crime even if they do not commit these crimes, which may partly be

responsible for the small effect. Those who do not have strong ICT skills seem to prefer traditional offending.

Gaming was related only to cyber-dependent offending. While there was no significant effect in the first model, controlling for environmental factors in the final model resulted in a marginally significant positive effect (p.<.10 instead of p<.05). Respondents who spend more time on gaming reported a greater variety of cyber-dependent offending.

Finally, we found a surprising effect of *positive cyber-behaviour*. This behaviour was positively related to all types of delinquency across all models, while the incidence rate ratios were also similar. In other words, respondents who reported more positive cyber-behaviour also reported a greater variety of cyber-dependent, cyber-enabled and traditional offending. While this seems counter-intuitive, it may also just show that rule-breaking is not as black and white as it may seem. Students in these schools may break the rules, but they still have the skills to help others, and that is what they appear often to do. Additionally, this result also suggests that these students are inclined to challenge themselves online. Sometimes they use their skills in illegal challenges, sometimes in legal challenges. As challenge has often been suggested as a motivation for cyber-delinquency, specifically for cyber-dependent offending, this result may be less surprising than it seems.

4.5.2 Results for environmental factors

In contrast to the findings about individual characteristics, the environmental factors included were found to be less related to *cyber-dependent* offending. Being at home alone, using a computer without supervision and talking about computer activities with teachers were found to be positively related in the first model, but these effects disappeared when controlled for individual factors in the final model. For *cyber-enabled* and *traditional offending*, on the other hand, environmental factors do seem to have an effect, independently both of each other and of the individual variables. Overall, the model fit for cyber-enabled and traditional offending improved when environmental factors were included in the final model, in contrast to the model fit for cyber-dependent offending. And for both types of offending, several environmental factors appear to have a statistically significant effect.

Offline rules by parents is significantly related to traditional offending, also in the final model. Respondents who reported more offline rules reported less traditional offending. *Online rules by parents* is significantly related to cyber-enabled offences, which suggests that respondents who report more online rules report less cyber-enabled offending. However, the effect is only marginally significant in the final model.

There are also some small effects of being at home alone and using a computer without supervision. *Being at home alone* has a small positive effect in both models on cyber-enabled behaviour. This means that respondents who spent more hours at home alone reported a greater variety of cyber-enabled offences. For *using a computer alone*, the significant positive effect in the first model disappeared in the final model for cyber-enabled offending. For traditional offending, we found only a trend (p <.10) for a negative effect in the final model. Although small and still uncertain, these effects suggest that opportunities for cyber-enabled offences may increase when other people are not present at home. For traditional offending, on the other hand, it seems less important, probably because opportunities for this type of offending mainly appear outside of the home in offline activities.

In addition to the home situation, the school seems to have an impact on cyber-enabled and traditional offending. However, both *online and offline rules of the school* are not related to cyber-enabled offending. For traditional offending, a positive effect (meaning more rules are related to more offending) was found in the first model, but this disappeared in the final model. A non-significant effect of online rules in the first model changed to a significant negative effect in the final model when controlled for individual factors. This indicates that respondents who reported more online rules at school reported a smaller variety of traditional offences. As respondents reported, on average, more offline than online rules, having online rules may be an indication that the school is stricter. This could explain why this factor has an impact on traditional offending. However, these rules do not seem to have an impact on cyber-offending.

School satisfaction and boredom have an effect on both cyber-enabled and traditional offending. For both types of delinquency, the effect of school satisfaction is stronger in the final model when controlled for individual factors. The effect indicates that respondents who reported greater school satisfaction reported a smaller variety of cyber-enabled and traditional offending. Similarly, being bored at school is positively related to both types of offending in the first model, indicating that respondents who are bored more often reported

more offences. However, this effect disappears in the final model. While these effects are in the direction that might be expected, the effect of *satisfaction with ICT education* is, as expected, in the opposite direction and, therefore, positively related to offending. For cyber-enabled offending, the effect was found to be significant in only the final model, whereas for traditional offending it was significant in both models. This indicates that respondents who reported more satisfaction with ICT education also reported a greater variety of cyber-enabled and traditional offending. The effect seems to be stronger for traditional offending. It should be noted that satisfaction with ICT education measured different aspects of satisfaction than the general school satisfaction variable because it also measured the extent to which students felt challenged and learned new skills at school. This may explain why this factor was also found to be related to traditional types of offending.

Lastly, *talking (with teachers) about computer activities* had a significant effect only for traditional and cyber-enabled offending in the first model. The effect indicates that respondents who reported a greater variety of offences also talked more about their online activities with their teachers. However, this effect disappeared in the final model when individual factors were included.

Table 11 summarises these results for the three different groups, based on the results in the final models, because these give the most comprehensive picture of the main independent effects. This table includes only personal characteristics and environmental factors significantly related to the type of offending. Factors included in red are negatively related, whereas factors included in green are positively related.

Table 11. Overview of significant results of full models

Cyber-dependent delinquency	Cyber-enabled delinquency	Traditional delinquency
INDIVIDUAL FACTORS		
- Age	- Age	- Age
+ Low self-control	+ Low self-control	+ Low self-control
+ Social skills	+ Social skills	+ Social skills
+ Computer addiction	+ Computer addiction	+ Computer addiction
+ ICT knowledge		- ICT knowledge
+ Positive cyber-behaviour	+ Positive cyber-behaviour	+ Positive cyber-behaviour
ENVIRONMENTAL FACTORS		
		- Offline rules by parents
	+ Home alone	
		- Online rules by school
	- School satisfaction	- School satisfaction
	+ ICT education satisfaction	+ ICT education satisfaction

red (-) = negative significant effect; green (+) = positive significant effect (p<.05)

4.6 Conclusion

This chapter presents the results for the first and fourth research questions: 'How are different types of cyber-delinquent behaviour among young people related to major individual characteristics and environmental factors?' and 'To what extent do these results differ between cyber-dependent, cyber-enabled and traditional delinquent behaviour?' In this conclusion we discuss the significant results in the final models that include both individual and environmental factors and focus on the two types of cyber-delinquency, and on the differences between them and traditional offending.

Overall the results show that cyber-dependent offences are mostly related to the individual factors included in this study, while cyber-enabled and traditional offences are also related to the environmental factors included in this study. Similar to other studies comparing factors related to these three categories of crime (Rokven, Weijters, & Van Der Laan, 2017), this indicates that cyber-enabled offending is more similar to traditional offending than cyber-dependent offending.

It should be noted, however, that the sample size and length of the survey limited the number of factors that could be included in these models. This means that not all other

factors, such as factors generally related to traditional offending, were included. Future comparisons including these variables may, therefore, find differences between cyber-enabled offending and traditional offending that were not found in this study. However, the study by Rokven et al. (2017) mainly used traditional risk factors, and found similar results.

Four individual characteristics – low self-control, good social skills, computer addiction and positive cyber-behaviour – were found to be positively related to all types of offending, although the strength of the effect sometimes varied. Age was negatively related to all types of offending. Not all these findings are in line with what could be expected. Firstly, cyber-offending, in particular cyber-dependent offending, could have been expected to require higher levels of self-control than traditional offending. Although some studies also found a positive relationship between low levels of self-control and cyber-offending (Bae, 2017; Weulen Kranenbarg, et al., 2021), other studies found or suggested a relationship between higher levels of self-control and particularly more technical and advanced forms of cyber-offending, given that these forms of offending would require attention and skills (see Van der Wagen et al., 2019). However, it is possible that the students in our sample (who were mainly following ICT programmes) may simply already have had enough skills to commit these crimes and so did not need the greater self-control required for the more advanced types of cyber-offending.

In addition, and in contrast to previous suggestions that cyber-dependent offenders had fewer social skills (Van der Wagen et al., 2019), all types of offending were found in our research to be positively related to social skills. This could indicate that all the types of offenders in our sample were actually more outgoing than the non-offenders. Again, our sample selection could have resulted in a more homogeneous group in this respect, given that the offenders and non-offenders in the sample were all following ICT programmes.

Another surprising result was that positive and negative cyber-behaviour were found to be related. This indicates that differentiating between 'good' and 'bad' students may not be as easy as it may seem. Gaming was only marginally significantly related to cyber-dependent offending; this result is not completely in line with more anecdotal evidence from previous studies that suggested a strong relationship between gaming and cyber-offending (see, for example, National Crime Agency, 2017).

With respect to environmental factors, rules and supervision by parents and schools and satisfaction with school or ICT classes or boredom at school appeared not to be related

to cyber-dependent offending. This suggests that this type of behaviour is more difficult for parents and schools to stop or reduce than cyber-enabled or traditional offending. For cyber-enabled offending, however, increasing online rules by parents and school satisfaction in general, and limiting the time spent at home alone, may be useful for reducing this behaviour. Interestingly, however, cyber-enabled offenders did feel challenged in ICT classes. These classes and the online rules at school would not appear, therefore, to be having the desired impact on cyber-dependent and cyber-enabled offending. While this study could not examine these ICT classes in detail, future qualitative studies may investigate how ICT teachers can influence students' online behaviour by reducing online offending while retaining or even increasing their positive cyber-behaviour.

5. Results: perceived and actual cyber-delinquent behaviour of friends[15]

5.1 Introduction

Now that we have examined individual characteristics and environmental factors in relation to cyber-delinquent behaviour, we focus on the role of friends. As discussed in Chapters 1 and 2, studies on the role of friends in cyber-delinquency are characterised by various limitations and shortcomings. The current and the next chapter address several of these shortcomings. To start with, our study included both perceptual and actual self-reported measurements of friends' delinquency, based on the friendship networks within the schools. This allowed us to investigate the discrepancy between perceived and actual cyber-delinquent behaviour of friends, and the extent to which both are related to cyber-delinquent behaviour of individuals. We also investigated whether the relationship between perceived cyber-delinquency of friends and someone's own delinquency varies between different types of friends (school friends, other offline friends and online contacts), and whether our findings varied between cyber-enabled, cyber-dependent and traditional delinquency.

This chapter provides answers to the second and fourth research questions: 'How is cyber-delinquent behaviour among young people related to actual and perceived cyber-delinquent behaviour of offline and online peers?' and 'To what extent do these results differ between cyber-dependent, cyber-enabled and traditional delinquent behaviour?' We test the following hypotheses:

- **Hypothesis 1:** Since it can be assumed that cybercrimes often take place in a highly anonymous context that can be easily hidden from the offline world, we expect the majority of respondents to have an inaccurate picture of their school friends' cyber-delinquency.
- **Hypothesis 2:** Because for traditional types of delinquency the relationship between individual offending and perceived offending of school friends (indirect measurements of delinquency) is generally stronger than the relationship between individual offending and actual self-reported delinquency of school friends (direct measurements of delinquency),

[15] This is a translated and revised version of a paper published in a Dutch journal (Van der Toolen, Weulen Kranenbarg, & Weerman, 2020).

we expect the relationship between perceived cyber-delinquency of school friends and individual offending to be stronger than the relationship between actual self-reported cyber-delinquency of school friends and individual levels of cyber-delinquency.

- **Hypothesis 3:** As previous research suggests that cyber-offenders often find information about offending online (Goldsmith & Brewer, 2015), and because online forums play an important role in the exchange of digital skills and opportunities (Holt, 2007; Hutchings, 2014), we expect the relationship between individual cyber-delinquency and cyber-delinquency of friends to be stronger for online friends than for offline friends.

5.2 Analytical strategy

Three types of variables were used: (1) *individual* self-reported delinquency of respondents, (2) *perceived* delinquency of respondents' school, offline and online friends (perceptual measurement of friend delinquency), and (3) *actual* self-reported delinquency of respondents' school friends (direct measurement of friend delinquency). How these were measured is described in Chapter 3. In the current chapter we used the self-reported delinquency measure from wave 1 instead of wave 2 (which was used in the previous chapter). There are some small differences in the measurements between these waves. In wave 1, for example, we also included questions about illegal gaming behaviour as part of the cyber-dependent delinquency measure.[16] For the cyber-enabled delinquency variable, we also asked more sub-questions for each type of offence in wave 1 (these were combined in wave 2). Table 2 in Chapter 3 provides an overview of all the remaining individual items for the delinquency measures in wave 1. As explained in Chapter 3, the delinquency variables (*cyber-dependent, cyber-enabled and traditional offending)* were constructed by summating the number of different types of offences committed in each delinquency category. They represent a variety measure.

For the perceptual measurement of friend delinquency, respondents were asked how many of their friends they believed had committed the main types of offences. As explained

[16] Specifically, we asked respondents whether they had ever: 1) tried to disrupt their game opponents' internet connection (e.g. by DDoS); 2) hacked into their opponents' game account, and 3) stolen any online goods (e.g. virtual coins or other online assets) from their opponent. This illegal gaming behaviour variable was not used in the other chapters.

in Chapter 3, offences were grouped together and respondents were asked about the offences committed by their school friends, their offline friends (friends outside school, for example from their neighbourhood or sports club) and friends with whom respondents only interacted online (e.g. through online gaming). They were asked to indicate, for each friend type, whether they thought that none of these friends (0), a few (1), approximately half (2), more than half (3), or all/almost all (4) of their friends had committed these offences (alternatively they could indicate that they did not know whether their friends had committed these offences). The perceptual measure was subsequently constructed by adding all perception scores for each of the three offence categories per friend type (see Chapter 3 for further details). A high value for these variables indicates that respondents believed that a relatively high number of their friends engaged in a category of delinquent behaviour. We also used a more basic measure that indicated whether respondents believed that *any of their friends* committed engaged in a category of delinquent behaviour. Scores were coded as missing when respondents 1) had indicated at least once that they did not know whether their friends committed a type of offence within a category, *and also* 2) never indicated that their friends had committed offence types within this category.

Social network data on school friends were used to construct the direct measurement of actual self-reported friend delinquency. When completing the questionnaire, all participants had access to a numbered list containing the names of all the respondents in their school who had pre-registered.[17] Respondents could list a maximum of ten school friends. Because all respondents also answered questions about their own delinquency, the information about the school friend network made it possible to calculate the extent to which each respondent had delinquent school friends. This was done by summating all individual delinquency scores of respondents' school friends for the three types of delinquency. A high score on these variables indicates that a respondent had many friends who had indicated that they had committed many offences within that delinquency category. These variables were coded as missing if a respondent did not specify any friends in the school network, *or* a respondent only specified friends who had missing values for the individual delinquency

[17] Sometimes students had not signed up in advance, but still wanted to participate when the investigator was present. The names and numbers of these participants were written down in a clearly visible place in the classroom (on a blackboard, for example). An advantage of this method is that it enabled the school networks included to be as complete as possible. A disadvantage, however, is that this method led to respondents who could not yet have been chosen as friends earlier that day being added to the friend pool during the day.

variables. Because this study's data collection was limited to schools, the actual self-reported delinquency of offline friends outside school and online friends could not be calculated.

In the analysis, we first describe the extent to which respondents had an accurate view of their school friends' offending, by comparing percentages of respondents believing that any of their school friends committed an offence category with the actual self reports if these friends. To investigate whether and to what extent there was a correlation between respondents' offending and both the indirectly (perceptual) and directly (actual self-reports) measured delinquency of their friends, Kendall's τ-b measures were used because these account for the skewed distribution of the variables. To compare these correlations with each other, Kendall's τ-b values were first transformed into Pearson's *r* (Walker, 2003: 526):

$$(1) \qquad r = \sin 0.5\,\pi \mathrm{t}$$

and subsequently into Fisher's *z* (Walker, 2003: 526):

$$(2) \qquad Z_r = 0.5 \log_e \frac{1+r}{1-r}$$

Then, based on Steiger's (1980: 245, 247) equations 3 and 10, and using software developed by Lee & Preacher (2013), we calculated whether the correlations for the perceptual and actual self-reported measurements of school friends' delinquency differed significantly from each other.

5.3 Results

Table 12 shows respondents' perception of the delinquency of their friends for each type of offence and each type of friend. Remarkably, for most of the offences, only a small proportion of respondents believed they had delinquent friends: the percentages fluctuated between 1.5 per cent (phishing by offline friends) and 16.2 per cent (traditional crimes committed by offline friends). It is also noticeable that a substantial part of the respondents indicated that they did not know how their friends behaved (about 15 per cent for each type of delinquency).

Table 12: Percentages pf respondent believing at least any of their school friends, offline friends and online friends committed offences

Category	Offence type	Friend type	% believed friends had committed offence	% believed friends had not committed offence	% don't know whether friends committed offence	% not applicable
CYBER-DEPENDENT	Hacking: guessing password	school	11.1	68.8	14.8	5.3
		offline	10.0	70.5	13.6	5.9
		online	9.0	67.6	14.3	9.1
	Hacking: technical aplications	school	8.0	73.3	18.7	0.0*
		offline	5.6	76.4	17.9	0.0*
		online	9.0	71.0	20.0	0.0*
	Stealing or damaging data	school	10.1	67.0	14.3	5.6
		offline	6.3	73.7	14.2	5.9
		online	7.2	69.5	15.0	8.3
	DDoS attacks	school	5.0	75.1	14.9	5.1
		offline	3.5	77.5	13.7	5.3
		online	7.1	71.0	14.1	7.9
	Malware	school	4.1	74.8	15.6	5.5
		offline	2.5	76.9	14.5	6.1
		online	3.2	73.3	15.4	8.1
	Cheating online gaming	school	7.2	70.8	17.9	4.2
		offline	6.1	72.0	16.8	5.2
		online	9.0	66.6	17.4	7.0
CYBER-ENABLED	Editing visual/audio files	school	7.8	73.1	14.9	4.3
		offline	7.1	73.5	14.7	4.7
		online	6.5	70.9	15.5	7.1
	Online conflicts	school	11.4	68.8	15.9	3.9
		offline	12.7	67.8	14.9	4.6
		online	9.7	67.5	15.6	7.2
	Online fraud	school	5.3	72.6	17.9	4.3
		offline	5.3	72.8	17.0	5.0
		online	4.7	69.7	18.0	7.5
	Illegal trade	school	3.5	76.0	16.8	3.7
		offline	5.3	75.1	15.3	4.3
		online	2.8	73.3	16.9	7.0
	Phishing	school	2.0	77.4	16.5	5.1
		offline	1.5	78.1	15.6	4.8
		online	1.7	74.2	17.0	7.1
TRADI-TIONAL	Theft, burglary, vandalism, violence, drug trade	school	9.6	68.6	17.6	4.3
		offline	16.2	64.2	14.9	4.7
		online	5.1	69.9	17.4	7.7

* Because of a programming error, the option 'Not applicable' was not available for this question. However, this did not have an impact on the results because 'don't know' and 'not applicable' were coded as the same category.

Tables 13 provide an overview of the perceptual (indirect) measurements per delinquency category compared to the actual self-reported (direct) measurement of respondents' school friends delinquency. These data need to be interpreted with caution: firstly, because schools always participated with a selection of students (a cohort of their students, or only the students enrolled in ICT programmes) and, secondly, because school networks were never complete, given that some students were absent when the questionnaire was being completed or were not willing to participate. Because the network data are incomplete, the direct measurements of school friends' actual self-reported delinquency are also limited. This is particularly problematic for seemingly 'false positives' (i.e. when students indicated that they believed they had school friends who engaged in a certain type of delinquency, but no friends in the school network self-reported that type of delinquency). It is possible that only the part of a respondent's school network in which no delinquency occurred was mapped, while the school friends who did not participate in the survey did commit offences. Therefore, Table 13 cannot provide reliable insight into the percentage of correct perceptions of friend delinquency, although the direct measurement does provide the lower limit of the prevalence of delinquent behaviour among a person's school friends. However, Table 13 can provide a conservative indication of the percentage of 'false negatives' (i.e. when students indicated that they believed that they did not have any school friends engaging in a particular type of delinquency, while some friends in the school network did actually report that behaviour). If at least one friend in the school network committed an offence, this already means that respondents were wrong to believe that their school friends did not exhibit that type of delinquent behaviour at all.

The dark grey areas in Table 13 represent the percentage of respondents who indicated that they did not have any delinquent school friends, but who, according to our network data, actually did have such friends. Thus, these dark areas give an indication of the 'false negatives' in our sample. These percentages are substantial for both cyber-dependent and cyber-enabled delinquency, with over a third of all respondents erroneously assuming that they did not have any delinquent school friends at all. The results for traditional delinquency were in line with these trends.

Table 13a: Comparison between perceptual (indirect) and actual self-reported (direct) measurement of cyber-dependent delinquency of school friends

	Delinquency - school friends (actual): % no delinquency	Delinquency - school friends (actual): % delinquency	Delinquency - school friends (actual): % missing
Delinquency - school friends (perceptual): no delinquency	6.0	38.6	7.9
Delinquency - school friends (perceptual): delinquency	1.2	18.4	2.6
Delinquency - school friends (perceptual): don't know	2.7	19.1	3.5

NOTE: Dark grey areas represent false negatives for respondents who reported no friend delinquency; lighter grey areas represent false negatives for respondents who indicated they did not know whether they had delinquent school friends.

Table 13b: Comparison between perceptual (indirect) and actual self-reported (direct) measurement of cyber-enabled delinquency of school friends

	Delinquency - school friends (actual): % no delinquency	Delinquency - school friends (actual): % delinquency	Delinquency - school friends (actual): % missing
Delinquency - school friends (perceptual): no delinquency	13.3	36.4	8.9
Delinquency - school friends (perceptual): delinquency	1.9	15.1	2.2
Delinquency - school friends (perceptual): don't know	5.4	13.9	2.8

NOTE: Dark grey areas represent false negatives for respondents who reported no friend delinquency; lighter grey areas represent false negatives for respondents who indicated they did not know whether they had delinquent school friends.

Table 13c: Comparison between perceptual (indirect) and actual self-reported (direct) measurement of traditional delinquency of school friends

	Delinquency - school friends (actual): % no delinquency	Delinquency - school friends (actual): % delinquency	Delinquency - school friends (actual): % missing
Delinquency - school friends (perceptual): no delinquency	21.3	37.6	9.8
Delinquency - school friends (perceptual): delinquency	1.2	7.2	1.1
Delinquency - school friends (perceptual): don't know	7.6	11.1	3.0

NOTE: Dark grey areas represent false negatives for respondents who reported no friend delinquency; lighter grey areas represent false negatives for respondents who indicated they did not know whether they had delinquent school friends.

The lighter grey areas in Table 13 show the percentage of respondents who indicated that they did not know whether they had delinquent school friends, but who, according to our network data, were friends with delinquent respondents. When the false negatives and these 'I don't know' values are added together, 57.7 per cent of the respondents misjudged their school friends' cyber-dependent delinquency, compared to 50.4 per cent for cyber-enabled delinquency. Traditional delinquency of school friends was misjudged by 48.7 per cent of the respondents.

Table 14 provides an alternative comparison by presenting the prevalence of delinquency among respondents and among school friends for the perceived (indirect) and actual self-reported (direct) measures. The table shows that 51.6 per cent of respondents reported having committed at least one cyber-dependent offence, compared to 35.0 per cent for cyber-enabled offences. The score for traditional delinquency was lower: 26.0 per cent reported at least one traditional offence. Once again, respondents' misperceptions about the delinquency of their school friends becomes clear. For example, only 22.3 per cent of the respondents indicated that they had school friends who committed cyber-dependent crimes, while, according to our network data, no fewer than 76.2 per cent of the respondents actually had school friends who reported a cyber-dependent offence themselves.

Table 14: Percentage of delinquent respondentsrespondents, delinquency of school friends (perceptual/indirectly measured) and delinquency of school friends (actual self-reports/directly measured) for cyber-dependent, cyber-enabled and traditional delinquency

	Delinquency - respondent %	Delinquency - school friends (perceived) %	Delinquency - school friends (actual) %
Cyber-dependent delinquency	51.6	22.3	76.2
Cyber-enabled delinquency	35.0	19.2	65.5
Traditional delinquency	26.0	9.6	55.9

The pattern for cyber-enabled offences is somewhat similar: 19.2 versus 65.5 per cent. The prevalence of traditional offences among school friends was also often misjudged: 9.6 per cent thought they had delinquent friends, whereas our data showed that, in reality, 55.9 per cent of the respondents had traditional delinquent friends in their school network.

These results show that respondents often have an incorrect perception about the delinquent behaviour of their school friends: they largely underestimate this delinquency. Although missing network information means that we cannot provide a definitive answer on the extent to which respondents have a false picture of their school friends' delinquency, all the results were in line with Hypothesis 1.

There were also differences between the three offence categories. As Table 13 cannot provide reliable insight into the percentage of correct friend delinquency perceptions, these differences can only be evaluated for false negatives. Table 13 suggests that respondents are more likely to misjudge their friends' involvement in cyber-dependent delinquency than their involvement in cyber-enabled and traditional delinquency. These differences in estimates were mainly caused by the number of respondents who did not know whether their school friends engaged in delinquent behaviour: this percentage was highest for cyber-dependent delinquency, and lowest for traditional delinquency.

Table 15 presents the correlations between the levels of individual self-reported delinquency and that of the individuals' school friends, directly measured using the social network information. Table 16 shows the correlations between individual delinquency and the perceptual measurements of school friends' delinquency. Because the distribution of the delinquency variables is skewed, we primarily looked at the Kendall's τ-b correlations to compare these two tables. We used the Fisher's Z scores to test whether the relationship between the perceptual measurements of school friends' delinquency was stronger than the relationship between the directly measured variables and individual delinquency (Hypothesis 2).

Table 15: Kendall's τ-b, Pearson's r and Fisher's z scores for the relationship between individual delinquency and delinquency of school friends (actual self-reports) for cyber-dependent, cyber-enabled and traditional delinquency

	Number of respondents	Kendall's τ-b	*p* (significance level)	*Pearson's r*	Fisher's *Z*
Cyber-dependent delinquency	761	0.192	<.001	0.297	0.306
Cyber-enabled delinquency	757	0.166	<.001	0.258	0.264
Traditional delinquency	755	0.169	<.001	0.262	0.269

Table 16: Kendall's τ-b, Pearson's r and Fisher's z scores for the relationship between individual delinquency and delinquency of school friends (perceptions) for-cyber-dependent, cyber-enabled and traditional delinquency

	Number of respondents	Kendall's τ-b	*p* (significance level)	*Pearson's r*	Fisher's *Z*
Cyber-dependent delinquency	664	0.406	<.001	0.595	0.686
Cyber-enabled delinquency	692	0.373	<.001	0.553	0.623
Traditional delinquency	695	0.357	<.001	0.532	0.593

Table 15 shows that the actual self-reported delinquency of school friends for cyber-dependent (τ=0.19), cyber-enabled (τ=0.17) and traditional delinquency (τ=0.17) was significantly (all p<.001) related to individual delinquency. In all three cases, this correlation was small (Kohler & Kreuter, 2009). Table 16 subsequently shows that the perceived delinquency of school friends was also significantly (all p<.001) related to the delinquency of individuals for all three offence categories: here, the correlations for cyber-dependent (τ=0.41), cyber-enabled (τ=0.37) and traditional delinquency (τ=0.36) are medium to strong (Kohler & Kreuter, 2009).

For both the cyber-dependent and cyber-enabled delinquency of respondents, the correlation with the perceptual (indirect) measurements of school friends' delinquency was significantly stronger than the correlation with the actual self-reported (direct) measurement (z = 8.30; p <.001 and z = 8.09; p <.001). This corroborates Hypothesis 2. The correlation between traditional delinquency of individuals and the perceived traditional delinquency of school friends was also significantly stronger than the relationship with the actual self-reported traditional delinquency of school friends (z = 7.04; p <.001). However, there were no clear differences in these relationships for cyber-dependent, cyber-enabled and traditional delinquency: all correlations were of similar strength.

Table 17 shows Kendall's τ-b correlations between individual delinquency levels and the perceptual measurements of peer delinquency for the different types of friends: school friends, other offline friends and online only friends. This table serves to evaluate Hypothesis 3, which stated that the relationship between individual cyber-delinquency and the perceptually measured cyber-delinquency of online friends is stronger than the relationship with cyber-delinquency of offline friends.

The table shows that, for cyber-dependent and cyber-enabled crime, the perceptual delinquency variables were significantly related to individual delinquency for all types of friends (p<.001), and in all cases the relationship was medium to strong. This also applied to traditional delinquency (p<.001). The variable with the strongest correlation with cyber-dependent delinquency of individuals was the perceived delinquency of school friends, but this correlation was not significantly stronger than the correlation with the delinquency of offline friends (z = 1.64; p =.10) and online friends (z = 1.64; p =.10). For cyber-enabled crimes, there was no correlation that was clearly the strongest, and we did not find any significant differences between the three types of friends. These findings do not, therefore, corroborate Hypothesis 3. For traditional delinquency, however, we did find significant differences: the correlation of the perceptual measure of friends' delinquency with individual levels was stronger for offline friends than for school friends (z = 5.14; p <.001) and online friends (z = 6.19; p <.001).

Table 17: Kendall's τ-b, Pearson's r and Fisher's z scores for the relationship between individual delinquency and delinquency (perceptions) of school friends, offline friends and online friends for cyber-dependent, cyber-enabled and traditional delinquency

	Friend type	Number of respondents	Kendall's τ-b	*p* (significance level)	*Pearson's r*	*Fisher's z*
Cyber-dependent delinquency	school	664	0.406	<.001	0.595	0.686
	offline	607	0.373	<.001	0.553	0.623
	online	573	0.373	<.001	0.553	0.623
Cyber-enabled delinquency	school	692	0.373	<.001	0.553	0.623
	offline	651	0.369	<.001	0.548	0.615
	online	615	0.372	<.001	0.552	0.621
Traditional delinquency	school	695	0.357	<.001	0.532	0.593
	offline	715	0.456	<.001	0.657	0.787
	online	666	0.333	<.001	0.500	0.549

5.4 Conclusion and discussion

This chapter investigated whether individual cyber-dependent and cyber-enabled delinquency were related to both actual self-reported and perceived delinquency of school friends, and to perceived delinquency of offline friends outside school and online friends. Firstly, we found that respondents often misjudged whether their friends were involved in cyber-delinquency. More than a third of the respondents believed that their school friends did not commit online crimes, while actually these friends did commit these crimes, and about a sixth of our respondents indicated that they did not know whether their friends engaged in cyber-delinquent behaviour. These misperceptions appear to be most pronounced for cyber-dependent delinquency, mainly because a relatively high number of respondents indicated that they did not know whether their friends were involved in this type of cyber-delinquency. Our results are therefore in line with Hypothesis 1 – the majority of respondents have an incorrect view of the cyber-delinquency of their friends. One possible explanation for this finding is that cyber-delinquency can easily be shielded from people's offline social environments (Jaishankar, 2008; Suler, 2004). However, it also possible that young people are not very aware of their friends' delinquency in general, since the respondents often also misperceived their friends' involvement in traditional delinquency.

Secondly, we found that perceptual measurements of friends' cyber-delinquency were significantly more strongly related to individual delinquency than direct measurements of friends' actual self-reported levels of cyber-delinquency, thus supporting Hypothesis 2. This is in line with previous findings for traditional delinquency (which were also corroborated by our findings). In general, this finding may either mean that young people more often adapt their behaviour to what they think about their friends' behaviour, or that they often assume that their friends behave in the same way as themselves.

Thirdly, perceptions of online friends' cyber-delinquent behaviour did not show a stronger relationship to individual cyber-delinquency than perceptions of the cyber-delinquency of school friends and other offline friends. This is in contrast with what we formulated in hypothesis 3. However, for traditional delinquency, we found the perceptions of offline friends' delinquency to be significantly more strongly related to individual traditional offending than both school friends' and online friends' perceived delinquency. Our analyses thus still point to a potential difference in the role of friends in traditional

delinquency compared to their role in cyber-delinquency. Whereas, in the case of cyber-delinquency, perceptions about friends within all types of friendships seem to play an equally important role, the role of offline friends in traditional delinquency may be the most important.

Various reasons may account for our finding, contrary to what we predicted in Hypothesis 3, that perceived delinquent behaviour of online friends is not more strongly related to cyber-delinquency than the perceived delinquency of offline friends. Firstly, by focusing on ICT schools, we selected a very specific sample. It is possible that, for this category of youths, school friends and perhaps also offline friends play a more important role in individual online delinquency than for youths who are not enrolled in ICT programmes. Another possibility is that online friends play a more important role in online delinquency for a select group of individuals who have a substantial part of their friendship network in the online world, but not for other groups of individuals. Future research should make a clearer distinction between people who report having many online friends versus people who report having no or few online friends, and between people for whom online friends play an important role in their lives versus people for whom online friends do not play an important role. Nevertheless, our analyses also suggest that, on average, the cyber-delinquent behaviour of online friends matters as much as that of school friends and offline friends. This also implies that interventions aimed at targeting the influence of friends' cyber-delinquency should focus on all types of friends, including online friends.

6. Results: Social network processes and actual cyber-delinquent behaviour of friends

6.1 Introduction

In the previous chapter we investigated relationships between someone's own cyber-delinquency and traditional delinquency, and the perceived and actual self-reported delinquency of different types of friends. These analyses were based on cross-sectional data collected during wave 1. In the current chapter, we employed longitudinal data to analyse relationships between actual self-reported delinquency of friends and individuals' own delinquency over time. This addresses one of the most pressing limitations in existing research on friends and cyber-delinquency: the lack of insight into the causal processes behind the relationship.

The current chapter provides an answer to the third and fourth main research questions: 'What is the causal relationship between actual cyber-delinquent behaviour of young people and that of their peers?' and 'To what extent do these results differ between cyber-dependent, cyber-enabled and traditional delinquent behaviour?' To answer these questions, we used the first two waves of social network data collected on school friends and their actual levels of cyber-delinquency. Sophisticated statistical methods (RSiena) allowed us to estimate the extent to which similarity in cyber-deviance between individuals and their friends was attributable to influence effects between the first two waves or to the selection of friends with similar behaviour, and thus whether there were indications that our respondents tended to adapt their delinquent behaviour to that of their friends, and whether they tended to become friends more often with classmates who were relatively similar to them with regard to delinquent behaviour. We tested the following hypotheses:

- **Hypothesis 1:** Based on previous social network research on traditional types of delinquency (see our literature review in Chapter 2), we can expect that there will be small peer influence effects, as well as peer similarity effects, for both types of cyber-delinquency and for traditional delinquency.
- **Hypothesis 2:** As previously indicated, cybercrimes take place in a highly anonymous context, and respondents generally have a more inaccurate picture of their friends' cyber-delinquency than of their friends' traditional delinquency, in particular in the case of

cyber-dependent offences (as demonstrated in the previous chapter). Therefore, we can expect that both influence and selection effects will be weaker for cyber-dependent and cyber-enabled delinquency of school friends than for traditional types of delinquency.

6.2 Analytical strategy

For this chapter, we used longitudinal data, collected in waves 1 and 2 of our study (before the COVID-19 lockdown). We included in our analyses the school network data for each of these waves, together with the self-reported delinquency measurements and a few other basic variables. The *network* data consisted of all the respondents' answers to the question of who their school friends were. They could choose a maximum of ten from a list of the other participants from their school. The *self-reported delinquency* measurements were, again, the number of different types of offences from the three delinquency categories we distinguished (cyber-dependent, cyber-enabled and traditional). Three *other variables* were included that we believed could be an important determinant of friendship selection: same gender, same school class and similarity in ICT knowledge. The first two are often included in network analyses similar to the one we conducted, while the third variable was included as a control in case this turned out to be an important selection criterion in our sample of students enrolled in ICT programmes. The measurements for the three types of delinquency and the other variables are described in Chapter 3.

To analyse how behaviour of individuals and their social network structures mutually affect one another, we employed stochastic actor-oriented modelling (SAOMs; see Snijders, 2001; Ripley, Snijders, & Preciado, 2020). To be precise, we used the SIENA method (Simulation Investigation for Empirical Network Analysis), which was run in the statistical program R (the RSiena software package; see Ripley et al., 2020). This is a statistical modelling method that enables researchers to investigate changes in both network structure and individual behaviour as joint dependent variables (Steglich et al., 2010). This meant we could estimate the determinants of friendship selection, as well as influences that friends have on behaviour.

In the modelling procedure, the total observed change (in friendship ties and in behaviour) between the first and the second measurement moment is modelled into small

basic changes ('micro-steps'). A network micro-step entails the breaking or making of one tie with another person (i.e., a friendship selection); a behaviour micro-step is a one unit change in the behavioural variable (in our case, one of the three delinquency measurements). The changes over time are modelled as a process in which sequential stages are dependent on the previous situation, and the sequences of these micro-steps are used to estimate the parameters in a simulation process (using a Markov Chain Monte Carlo approach). Network dynamics and behavioural changes are modelled simultaneously by taking the estimated state of the network in each step as input for the behavioural changes and vice versa (for more details, see Snijders et al. 2010; Ripley et al. 2020). Parameter sizes and standard errors are estimated by comparing the simulations with the observations within each wave. This is repeated in iterative steps until a satisfactory fine-tuning of values is reached ('convergence').

The sample for the current study consisted of 18 school *cohorts* with students from the same grade.[18] However, not all these cohorts were sufficiently well equipped to be included in the network analysis used for this chapter. In a number of cohorts, too few respondents participated in the two waves of the survey, or a too small proportion of the total cohort. In both cases, it was not possible to conduct meaningful analyses of the total network, either because of a lack of statistical power, or because a too large proportion of the network was missing. The RSiena calculations for these networks did not result in converging estimations. For cyber-dependent and traditional delinquency, 13 of the school cohorts were included in the calculations where convergence was reached for the estimations of the parameters. For cyber-enabled delinquency, convergence could not be reached for two additional cohorts, which were therefore left out of the final calculations for this type of offending.

RSiena analyses for the three types of delinquency were run for each of the school cohorts separately, and the parameter estimates were subsequently combined by conducting a random-effects meta-analysis using the *metafor* package (see, for a script example, Snijders, 2020; for the *metafor* package, see Viechtbauer, 2011). This module estimates and tests average effects and standard errors, as well as indicators of variance across networks. For

[18] Note that a total of 12 schools participated in our study. However, instead of automatically modelling a school as one network, we distinguished, if applicable, cohorts that existed within the schools. If, for instance, a school participated with both first-year and second-year students, we distinguished two cohorts within this school: a first-year cohort, and a second-year cohort. All schools participated with either one or two cohorts.

three school cohorts, the estimation for the 'same gender' effect was always left out because these cohorts consisted only of boys.

The number of parameters that can be included in these kind of models is necessarily restricted in order to retain statistical power and to reach convergence. Our choice of parameters was based on previous social network research and our main interest in estimating selection and influence effects with regard to delinquency.

Effects on changes in friendships were estimated in the network dynamics part of the SIENA modelling procedure. We included several effects on friendship selection that are standard or recommended in the literature and the RSiena manual (see Ripley et al., 2020; Veenstra & Dijkstra, 2011). Firstly, we estimated various structural network effects that are often reported to contribute to network evolution. This included the basic outdegree effect (i.e. the baseline probability of making ties with others), the effects of reciprocity (i.e. choosing someone who has already chosen you), the 3-cycles effect (i.e. the tendency to close the cycle in a group of three, so that each person chooses another), the gwesp effect (i.e. a generalised tendency to choose someone who is also chosen by a friend) and the indegree popularity effect (i.e. choosing someone who is relatively often chosen as a friend; also referred to as the Matthew effect). Secondly, we included selection effects based on similarity in gender (boys tend to choose boys; girls tend to choose girls), being in the same school class (a group of students who usually follow education together, and therefore are also more likely to befriend each other) and similarity in ICT knowledge. Thirdly, we included a number of selection effects based on delinquent behaviour: whether there is an increased chance of selecting friends who report high numbers of delinquent behaviour (delinquency alter), an increased chance of selecting friends if you report high delinquency yourself (delinquency ego) and an increased chance of selecting friends who are relatively similar in delinquent behaviour to yourself (delinquency similarity). The latter parameter represents the classic *peer selection effect* that we were interested in.

Effects on changes in offending were estimated in the behavioural part of the model. Firstly, we included two basic parameters representing the general trend in offending behaviour over the two waves of the study: the 'linear shape', which is a baseline estimation of the average tendency over the research period, and the 'quadratic shape', which indicates the effect of initial offending behaviour on itself (positive if respondents tend to become more extreme in their behaviour over time: negative if behaviour tends to develop towards average

levels over time). Secondly, we included a parameter for the effect of ICT knowledge on behaviour so as to control for the possibility that this characteristic would bias the effects of cyber-delinquent friends. Thirdly, we included the 'total similarity' effect, which estimates the extent to which respondents adjust their offending towards the total level of delinquency of their school friends in the network. In other words, this estimates the extent to which respondents become more similar to the total level of delinquency of their alters, and this represents the *peer influence effect* we were interested in. Instead of total similarity, we could also have used the average similarity effect parameter. Runs with this option resulted in basically similar results, but less satisfactory model convergence.

6.3 Results

Table 18 shows the results of our RSiena analysis for cyber-dependent delinquency. We present the estimates of the effect sizes on changes in friendship selection and behaviour, the standard error and p-value of this estimate, the Q value that indicates variance (or heterogeneity) between school cohorts and its p-value, and the number of cohorts that were included in the calculation of the estimates.

The first part of the table presents the results on network dynamics. The basic rate for this indicated that, between the waves, there were on average six changes in friendship nominations in the simulation model. The next five structural network parameters were all found to have a significant effect on friendship selection, which confirms that these common network processes were also active among the young students with ICT education in this study. These students tended: to choose not everyone from their cohort (negative outdegree), to mirror friendship nomination to them (reciprocity), to complete friendship cycles (3-cycles and gwesp effect) and to select friends often chosen by others (indegree popularity). They also tended to choose fellow students from the same gender and the same school class. However, the estimated tendency to choose others with similar levels of ICT knowledge was not statistically significant.

Table 18: Outcomes of the RSiena analysis (multi-group estimates) for cyber-dependent delinquency

Variable	Estimate effect size	Standard error	p. (significance level)	Q value (variance)	p. of Q	Number of groups
NETWORK DYNAMICS (EFFECTS ON FRIENDSHIP SELECTION)						
Basic rate parameter[19]	6.533	0.776		58.430	0.000	13
Outdegree (density)	-2.299	0.186	0.000	24.702	0.016	13
Reciprocity	1.727	0.161	0.000	35.402	0.000	13
3-cycles effect	-0.142	0.063	0.024	25.967	0.011	13
Gwesp effect	1.737	0.124	0.000	23.197	0.026	13
Indegree popularity	-0.209	0.033	0.000	23.45	0.024	13
Same gender	0.200	0.062	0.001	3.701	0.930	10
Same school class	0.765	0.139	0.000	39.026	0.000	13
ICT knowledge similarity	0.257	0.215	0.233	22.775	0.030	13
Cyber-dep. delinquency alter	0.044	0.030	0.147	5.783	0.927	13
Cyber-dep. delinquency ego	-0.027	0.038	0.486	13.997	0.301	13
Cyber-dependent delinquency similarity	0.079	0.384	0.837	6.006	0.916	13
BEHAVIOURAL DYNAMICS (EFFECTS AND FRIENDSHIP INFLUENCE ON BEHAVIOUR)						
Basic rate cyber-dep. delinquency	5.121	1.037		23.998	0.020	13
Linear shape	-0.506	0.077	0.000	23.879	0.021	13
Quadratic shape	0.040	0.009	0.000	9.684	0.644	13
Effect of ICT knowledge	-0.035	0.030	0.239	8.966	0.942	13
Cyber-dependent delinquency total similarity	-0.155	0.241	0.519	5.442	0.706	13

The last three rows of the network dynamics show the friendship nomination effects with regard to cyber-dependent delinquent behaviour. Here, the estimated values for alter and ego levels, as well as for similarity, were relatively small and statistically non-significant. This means that, contrary to Hypothesis 1, we did not find a selection effect for this type of delinquency.

The second part of the table shows the results with regard to the behavioural dynamics. The basic rate indicates the average number of changes in the level of cyber-dependent delinquency in the simulation model. The negative linear shape shows that respondents tended to decrease their level of involvement between waves. The small quadratic shape effect shows that respondents tended to become more pronounced in their behaviour over time (those with high levels tended to increase, whereas those with low levels

[19] Basic rate parameters do not require a significance test because they are necessarily different from zero.

tended to decrease their involvement in cyber-enabled delinquency). We did not find an effect of ICT knowledge on changes in cyber-dependent delinquency, which confirms the previous cross-sectional findings reported in Chapter 4. Of most interest in this part of the table is the last row: the influence of the total involvement levels of friends on changes in an individual's own cyber-dependent delinquency. Again, we did not find a statistically significant effect for this. Although the estimated value here is negative, the standard error is substantial, which means that the true direction of this effect is highly uncertain and we cannot tell whether it is different from zero. This result is also contradictory to Hypothesis 1 (we had expected small peer influence effects, alongside peer similarity effects, for both types of cyber-delinquency and for traditional delinquency).

The findings with regard to variance show that, for most standard effects of the model, there was considerable heterogeneity between school cohorts. These subsamples differed in the extent to which friendship networks were shaped according to structural network processes and the level and trend of delinquent behaviour. The friendship selection effect of similarity in ICT knowledge also seemed to vary between school cohorts (perhaps related to differences in the type of education). However, no significant heterogeneity was found with regard to the effects we were mainly interested in. This suggests that our failure to find support for Hypothesis 1 was not due to important differences between school cohorts.

Finally, an interesting result is that we found no heterogeneity between school cohorts in the effect that being of the same gender has on friendship selection. This means that, in all cohorts, there was a similar tendency for boys to choose boys and for girls to choose girls. Note that this estimate is based on ten schools instead of thirteen – three schools were not included because they had too little variation in gender composition (these schools consisted entirely, or almost entirely, of boys).

Table 19 shows the results of our RSiena analysis for cyber-enabled delinquency. The findings with regard to the structural network effects were basically the same as in the previous model. Again, having the same gender and being in the same school class were found to have important effects on the probability of becoming friends. The estimated effect of similar levels of ICT knowledge may be substantial, but did not reach the border of statistical significance. For cyber-enabled delinquency, the three friendship nomination effects were not statistically significant, just as we saw for cyber-dependent offences. This is again in contradiction to Hypothesis 1. It should be noted, however, that the ego effect (i.e. more

delinquent respondents choose more friends in general) was closer to significance. It should also be noted that the selection effect of similarity in offending was found to be quite substantial, but not statistically significant, given that the standard error was also high.

Table 19: Outcomes of the RSiena analysis (multi-group estimates) for cyber-enabled delinquency

Variable	Estimate effect size	Standard error	p. (signi-ficance level)	Q value (variance)	p. of Q	Num-ber of groups
NETWORK DYNAMICS (EFFECTS ON FRIENDSHIP SELECTION)						
Basic rate parameter	6.720	0.600		25.124	0.005	11
Outdegree (density)	-2.478	0.200	0.000	14.637	0.146	11
Reciprocity	1.735	0.174	0.000	23.617	0.009	11
3-cycles effect	-0.105	0.067	0.115	20.166	0.028	11
Gwesp effect	1.697	0.123	0.000	11.636	0.310	11
Indegree popularity	-0.201	0.037	0.000	18.399	0.049	11
Same gender	0.237	0.074	0.001	4.649	0.864	10
Same school class	0.659	0.154	0.000	30.951	0.001	11
ICT knowledge similarity	0.262	0.181	0.148	12.941	0.227	11
Cyber-enabled delinquency alter	0.080	0.082	0.328	5.716	0.839	11
Cyber-enabled delinquency ego	0.113	0.070	0.104	1.982	0.996	11
Cyber-enabled delinquency similarity	0.639	0.561	0.254	4.895	0.898	11
BEHAVIOURAL DYNAMICS (EFFECTS AND FRIENDSHIP INFLUENCE ON BEHAVIOUR)						
Basic rate cyber-enabled delinquency	2.572	0.349		8.014	0.628	11
Linear shape	-0.827	0.146	0.000	16.524	0.086	11
Quadratic shape	0.151	0.035	0.000	3.199	0.976	11
Effect of ICT knowledge	-0.040	0.075	0.589	12.21	0.271	11
Cyber-enabled delinquency similarity	-0.277	0.222	0.212	2.741	0.987	11

The results with regard to the behavioural dynamics were largely similar to those reported for cyber-dependent delinquency. The quadratic shape effect was a bit larger, meaning that respondents substantially tended to become more pronounced in their behaviour (i.e. those with high levels tended to increase, and those with low levels tended to decrease their involvement in cyber-enabled delinquency). Again, the effect of cyber-enabled delinquency

of school friends was negative, but statistically not significant. This means that here, too, we found no support for Hypothesis 1.

Table 20 shows the results of our RSiena analysis for traditional types of delinquency. Not surprisingly, the estimated effects for most network dynamic effects were almost identical because these were included in both analyses. This table also shows friendship selection to be largely governed by structural network effects and a preference for friends of the same gender and in the same school class.

Table 20: Outcomes of the RSiena analysis (multi-group estimates) for traditional delinquency

Variable	Estimate effect size	Standard error	p. (signi-ficance level)	Q value (variance)	p. of Q	Num-ber of groups
NETWORK DYNAMICS (EFFECTS ON FRIENDSHIP SELECTION)						
Basic rate parameter	6.369	0.644		50.066	0.000	13
Outdegree (density)	-2.440	0.171	0.000	18.509	0.101	13
Reciprocity	1.678	0.151	0.000	33.648	0.001	13
3-cycles effect	-0.110	0.059	0.063	26.349	0.01	13
Gwesp effect	1.696	0.114	0.000	20.842	0.053	13
Indegree popularity	-0.196	0.036	0.000	33.525	0.001	13
Same gender	0.203	0.064	0.001	4.776	0.906	10
Same school class	0.774	0.160	0.000	35.766	0.000	13
ICT knowledge similarity	0.204	0.157	0.192	15.909	0.195	13
Traditional delinquency alter	0.058	0.082	0.478	2.474	0.998	13
Traditional delinquency ego	0.005	0.082	0.954	7.075	0.853	13
Traditional delinquency similarity	0.751	0.421	0.075	3.203	0.994	13
BEHAVIOURAL DYNAMICS (EFFECTS AND FRIENDSHIP INFLUENCE ON BEHAVIOUR)						
Basic rate traditional delinquency	1.827	0.263		8.488	0.746	13
Linear shape	-1.401	0.350	0.000	28.204	0.005	13
Quadratic shape	0.300	0.090	0.001	12.835	0.381	13
Effect of ICT knowledge	-0.057	0.070	0.412	7.350	0.864	13
Traditional delinquency total similarity	-0.250	0.240	0.298	6.901	0.834	13

With regard to the friendship selection effects based on delinquent behaviour, the results of Table 20 show no statistically significant effect of ego and alter levels of traditional offending

on the number of friendship nominations. However, the effect of similarity in traditional delinquency was now more substantial and reached one-sided statistical significance (p.<10). This means that the selection effect of friends' traditional delinquency was somewhat stronger than for both types of cyber-delinquency, which is in line with Hypothesis 2.

The findings on the behavioural dynamics for traditional delinquency showed a relatively low base rate, with a tendency to decrease offending, but the quadratic shape had an even stronger effect than for cyber-enabled delinquency (tendency away from the average score). Here, too, the influence effect of total traditional delinquency levels of friends was negative, but statistically not significant. This is somewhat surprising in the light of most recent research using social network techniques. It means that, in the case of influence effects, Hypothesis 2 is not supported: for all types of offending, we found no clear influence effect of delinquent behaviour of school friends.

6.4 Conclusion and discussion

In this chapter, we employed longitudinal social network data to investigate whether there were indications that school friends influenced each other's cyber-delinquency by adapting their level of involvement over time, and whether there were indications that students selected each other as school friends based on similarity in cyber-delinquent behaviour. The answers to these questions can provide insight into the causal direction of the relationship between actual cyber-delinquent behaviour of young people and that of their peers.

For both cyber-dependent and cyber-enabled delinquency we found no clear and statistically significant indication that respondents chose their school friends based on their level of offending. All the basic network processes were in place and students were found to have a preference for making friends with other students from the same gender and the same classroom, but did not show a tendency to choose friends with levels of cyber-offending that were high or similar to their own. This was not in line with Hypothesis 1 – we had expected at least some degree of peer similarity in cyber-delinquent behaviour.

We also did not find an influence effect for cyber-delinquent behaviour. Our respondents did not significantly tend to adapt their offending towards the total level of cyber-delinquency of their school friends, controlled for previous levels and general trends.

As we had expected at least some effect, based on previous network research on peers and delinquency, this finding is also in contradiction to Hypothesis 1. The actual delinquency of school friends would appear not to play an important role in increases and decreases over time in someone's own involvement in cyber-delinquency, and this remains to be explained by other factors.

For traditional types of delinquency, we found indications that respondents tended to make friends at school with others who were similar in offending levels, but we did not find an influence effect for delinquent school friends. This is partly in line with Hypothesis 2 – the peer selection effect for traditional delinquency was stronger than for cyber-delinquency. The lack of an influence effect for traditional delinquency, too, differs from the results in most previous studies using this analytical method.

There may be a variety of explanations for the failure to find clear selection and influence effects for the two types of cyber-delinquency. Firstly, the correlation we found in Chapter 5 between actual cyber-delinquency of school friends and that of the respondents themselves may have been largely spurious. Other network processes and preferences (e.g. that boys tend to befriend boys) may be at least partly responsible for the friendships between cyber-delinquent respondents at school. Secondly, other variables, which were not included in the analysis, may be more important than we had thought. For example, parenting practices, school performance and individual characteristics might influence cyber-delinquent (and traditional delinquent) behaviour, but also preferences for making friends with others. And changes in these circumstances and personal characteristics may also explain the short-term changes (over a few months) in delinquent behaviour that we investigated in this chapter. Thirdly, the short-term changes in cyber-delinquency may also be caused by relatively coincidental opportunities encountered online, or be informed by online information that respondents retrieved themselves. In that case, school friends would not matter much for behaviour. Fourthly, it is also possible that no selection and influence effects exist with regard to school friends, but that such effects do exist for other types of friends, in particular online friends. Future research on offline and online activity and communication is needed to investigate this possibility.

7. Conclusions and implications

7.1 Background

As cybercrime accounts for a substantial component of juvenile delinquency, it is crucial to have a good understanding about this type of offending. In comparison, however, to traditional delinquency, we know very little about cybercrime among juveniles from previous research. It was unclear, for example, which personal and environmental factors related to cyber-delinquency and whether these factors were the same as or different from those relating to traditional delinquency. This report therefore examined which individual characteristics and environmental factors related to cyber-offending, with a specific focus on the importance of peer relationships. While the role of peers has been studied before, previous research on cyber-delinquency relied mostly on cross-sectional data and perceptual measures of peer delinquency. These studies were unable to examine the extent to which juveniles actually knew whether their peers had committed cybercrimes. There was previously also no research on causal relationships that distinguished between selection and influence processes. In addition, comparisons between online and offline peers were scarce.

Consequently, we conducted a longitudinal study (in three waves) among a substantial sample of Dutch secondary and tertiary school students considered to be at an elevated risk of committing cyber-offences (i.e. ICT students or students following ICT tracks or courses). We collected self-report data on a large variety of cyber-offences, and on different categories of offline and online peers. We also collected survey data on several individual characteristics and environmental factors and detailed social network data on the respondents' school friends. This final chapter discusses our findings for the five overarching research questions. The detailed results can be found in chapters 4 – 6. In the current chapter we discuss general conclusions and their implications (in particular with regard to prevention and intervention) and relate these to the insights from the expert meeting.

7.2 Conclusions on research questions

The first result to be mentioned is that a substantial proportion of our respondents were involved in some form of cyber-delinquency, either cyber-dependent and/or cyber-enabled. About half of them indicated that they had committed a cyber-dependent offence in each wave, and more than one in three that they had committed a cyber-enabled offence. The most prevalent cyber-dependent offences were vandalising data and hacking by guessing a password. More technical cyber-dependent offences, such as hacking by using technical applications or exploits, were also quite common in this sample. The most prevalent cyber-enabled offences were fighting out conflicts online and online fraud. Juveniles in our sample were even more involved in cyber-delinquency than in traditional delinquency. These figures illustrate that our respondents (students in ICT programmes) indeed constitute a sample with a relatively high risk of cyber-offending.

7.2.1 Cyber-delinquent behaviour and its risk factors

With regard to the first and fourth research questions – 'How are different types of cyber-delinquent behaviour among young people related to major individual characteristics and environmental factors?' and 'To what extent do these results differ between cyber-dependent, cyber-enabled and traditional delinquent behaviour?' – our results showed that cyber-dependent offences are mainly related to the individual factors investigated, while cyber-enabled and traditional offences are also related to the environmental factors we included in this study. This suggests that cyber-enabled offending is more similar to traditional offending than cyber-dependent offending, as also found in previous research on cyber-offenders (Rokven et al., 2017). This implies that, in the case of cyber-dependent offending, it may be more difficult for parents and schools to halt this type of behaviour. For cyber-enabled offending, however, results suggest that increasing online rules by parents, enhancing school satisfaction and limiting the time spent at home alone may help to reduce this behaviour. However, providing challenging ICT classes and increasing online rules at school do not seem to have the potential to impact on cyber-dependent and cyber-enabled offending.

The individual factors of low self-control, computer addiction, good social skills and positive cyber-behaviour were positively related to all types of offending. ICT knowledge was significantly related only to cyber-dependent offending, confirming evidence from previous studies (see, for example, National Crime Agency, 2017). The finding that cyber-dependent delinquency was related to low self-control is notable, since some previous studies found that these more advanced types of crimes require higher levels of self-control (see Van der Wagen et al., 2019). We believe this finding may be explained by the special nature of our research sample: the students sampled may already have had enough skills to commit these crimes and so did not need more self-control for the more advanced types of cyber-offending. Another surprising finding was that all types of offending were positively, and not negatively, related to good social skills. This again may be traced back to the special nature of our sample. Future research on more general samples will be needed to obtain more clarity on these issues. We were also surprised that cyber-delinquency was substantially related to positive cyber-behaviour, indicating that differentiating between 'good' and 'bad' students is not as easy as it may seem: students who are active online may exhibit both types of behaviour.

The experts that we talked to reported that they had seen evidence of the effects of low self-control, computer addiction and gaming in their day-to-day work. They suggested that the surprising positive association between good social skills and cyber-offending indicated that different categories of offenders could be identified. Some young cyber-offenders may be 'lone actors' (which is the general picture of these offenders; see Van der Wagen et al., 2019), while others may be very outgoing. With respect to the surprising association between cyber-delinquency and positive cyber-behaviour, the experts suggested that this could be explained by some of these ICT students having a general interest in online behaviour. This category of students may not have known when they were crossing a line while acting online, and the question of whether their behaviour was legal or illegal may depend on the situation.

7.2.2 Perceived and actual cyber-delinquent behaviour of friends

With respect to our second and fourth research questions – 'How is cyber-delinquent behaviour among young people related to actual and perceived cyber-delinquent behaviour of offline and online peers?' and 'To what extent do these results differ between cyber-

dependent, cyber-enabled and traditional delinquent behaviour?' – it became clear that respondents often misjudged whether their friends were involved in cyber-delinquency, particularly in the case of cyber-dependent delinquent behaviour. In about half the cases, respondents were not aware of their school friends' cyber-delinquent behaviour. In comparison to the actual self-report (direct) measures of peer delinquency, perceptual (indirect) measures of friends' cyber-delinquency were more strongly related to an individual's own cyber-delinquency. This suggests that young people may often adapt their cyber-behaviour to how they *believe* their friends behave. This makes sense, as it is easy for friends to shield the kind of delinquent behaviour they actually engage in online (Jaishankar, 2008; Suler, 2004).

In the case of cyber-delinquency, perceptions about online friends were equally related to the cyber-delinquency of an individual as perceptions about offline friends were. Although we expected online friends to be more important, this finding was still different from our findings for traditional delinquency. For traditional delinquency, the relationship was the strongest for the perception of offline friends' delinquency (compared to the perceived delinquency of online friends and school friends).

7.2.3 Social network processes related to actual cyber-delinquent behaviour of friends

With regard to the third and fourth research questions – 'What is the causal relationship between actual cyber-delinquent behaviour of young people and that of their peers?' and 'To what extent do these results differ between cyber-dependent, cyber-enabled and traditional delinquent behaviour?' – we did not find much evidence for substantial effects. There were no clear indications that actual cyber-delinquency of school friends led to a change in individuals' own cyber-delinquent behaviour over a period of a few months. We found a general trend that respondents' involvement decreased between the two waves, but also that juveniles already involved in high levels of cyber-delinquency committed even more offences in the second wave. What caused these short-term changes in cyber-behaviour remained unclear, however. Further research is consequently needed to shed more light on this.

We also did not find any clear indications that cyber-delinquent behaviour was important for selecting school friends. In general, respondents were found to choose their

friends based on gender or on general network mechanisms (e.g., choosing friends of friends, or selecting the more popular students). Traditional types of delinquency may be important as a criterion for selecting friends, but cyber-delinquency would not appear to be. This finding may be explained by the low visibility of cyber-delinquency: respondents simply do not really know whether their school friends are involved in this form of delinquency, as already demonstrated by our finding that perceptions of peers' cyber-delinquency may matter more than actual cyber-offending.

The combined findings about causal processes and the different measurements of peers' cyber-delinquency imply that focusing on school friends' direct influence on juvenile cyber-offending would not seem to be very important. Although it is not certain whether this also holds true for other types of friends (i.e. outside school), we have no reason to believe that it would be much different. Instead, it might be more fruitful to devote attention to young people's perceptions about their friends. Teaching about the moral boundaries of online behaviour and the negative consequences of cyber-offending might be a useful way of making young people more resistant to imitating friends whom they believe to be involved in cyber-offending.

7.3 Limitations and suggestions for future research

This study addressed several limitations of previous research on cyber-delinquency. However, it also has its own limitations. Future research may improve our insights with regard to the studied sample, the data collected on peers, the number of waves, and the breadth and depth of the information collected.

With regard to the sample, our choice to focus on a relatively high-risk group of youths was unique and different from previous research. The fact that cyber-offending was very common in this group offers important insights into how delinquency in this group can be explained and prevented. However, the results may not necessarily be generalisable to students in this age group in general or to students in other countries. For example, our surprising results with respect to social skills and ICT knowledge may be attributable to the high-risk nature of the sample and may be found to differ if these aspects are studied in the population in general. Future research with more representative samples of youths (or

students in other types of ICT education, such as higher tertiary education) in various countries should test whether these findings remain similar. These studies will need, however, to be large enough to include a substantial portion of cyber-delinquent students. In addition, the participants at the expert meeting emphasised that knowledge about older offenders remains limited, thus suggesting that future studies should also include looking at predictors of cyber-offending among adults.

In our study, we gathered unusually detailed self-report data about different types of cyber-offending. When analysing this report we grouped these offences into two broad categories: cyber-dependent and cyber-enabled offending. This meant we could not differentiate between less serious and more serious levels of offending within these categories, and it is possible that the relationships we found may differ between those committing minor cyber-offences and those committing cyber-offences of a more serious nature. However, we did a robustness check to see whether our results on the major relationships were driven mainly by the most prevalent but relatively minor cyber-offences of guessing passwords or having online conflicts. This was found not to be the case: the results were largely the same when these two offences were removed from the analysis. Nevertheless, future research could choose to analyse relationships of individual characteristics and environmental risk factors in more detail, and specifically to distinguish between minor cyber-offences and more serious cyber-offences. These future studies could also include additional characteristics and risk factors, given that we included only a selection of the most frequently mentioned variables from the literature on cybercrime.

With respect to the role of peer delinquency, this is the first study to directly measure the cyber-delinquency of friends. However, we only collected data on social networks in schools. Therefore, our direct measures of actual self-reported delinquency were limited to school friend delinquency. To investigate the differences between actual self-reported and perceptual measurements of friend delinquency in more depth, it would have been interesting also to have included respondents' offline out-of-school and online friend networks. This would be a complicated endeavour because including the majority of a friendship network outside school in a study is difficult, albeit not impossible (see Burk, Steglich, & Snijders, 2007). With regard to our own study, the need to obtain permission from parents for students aged under sixteen resulted in a substantial loss of respondents and in incomplete friendship networks at some schools. As this permission is now required

throughout the EU, future studies with a similar approach are likely to face similar problems. In many previous studies, by contrast, it was possible to operate an 'opt-out system' (i.e. parents had to take action to indicate that participation was viewed as undesirable) rather than an 'opt-in system' (where parents had to actively confirm that their children had permission to participate), and this generally resulted in high participation rates across schools. A final remark with respect to our focus on peer delinquency is that we did not study the overlap in the effects of school friends, offline friends and online friends, and nor did we study online and offline communications with friends. Future research could investigate whether and how these factors, in concert, affect the influence of friend delinquency.

Because of the COVID-19 pandemic and the fact that we had to move our final wave online, we suffered a substantial loss of participants in this third wave. Therefore, our analyses had to be restricted to data from the first two waves. Although conducting longitudinal network analysis in just two waves is perfectly possible, including a third wave would have increased the power of our analyses. Furthermore, several potential predictors of cyber-offending, such as the perceptions of the risk of getting caught, were only included in the third wave. We were consequently unable to study these variables in relation to offending with enough statistical power. These factors should therefore be included in future research and could answer additional questions about deterrence that were raised during the expert meeting.

Our quantitative focus and the need to choose which questions to include in the surveys limited us in the extent to which we could examine factors and processes related to cyber-delinquency. Our results suggested, for example, that online friends were just as important as offline friends. It would have been valuable, therefore, to have been able to find out how students were using platforms such as online forums. Do they use these solely as one-way sources of information, or do they meet and interact with online friends on these platforms? Similarly, to what extent do students learn about cyber-delinquency from their offline or online peers, or from online sources? In addition, it would be interesting to examine what students actually see or know about the online behaviour of their peers, and the extent to which this differs between different types of peers. These questions could be addressed in future surveys or in qualitative studies seeking to gain a deeper understanding of the underlying processes.

Apart from these suggestions linked to limitations in our methodology, the experts raised several other ideas for future research that would help them to prevent cyber-delinquency. As mentioned above, perceptions of the risks of getting caught and deterrence were considered to be important topics for future research. The experts we consulted emphasised that online monitoring was not exclusively the task of the police, and mentioned that they would like to learn more about the extent to which students felt that their online behaviour was monitored by different types of actors. The experts also wondered about the extent to which students were aware of the rules and knew when they had crossed a line online and what the consequences would be if they were caught. It may also be valuable to investigate students' norms on online behaviour, and how friends or online communities may influence these norms. Another interesting question raised concerned the circumstances in which students showed positive cyber-behaviour and those in which they showed negative cyber-behaviour.

The experts also reiterated that there may be several different types of offenders, each, for example, with their own different motives and skills. Future studies should distinguish between these types and investigate any differences. And, lastly, a general remark by the experts was that there was a need for experimental studies on prevention, to test what works in preventing cybercrime, and what does not.

7.4 Practical and policy implications

This section addresses our fifth and final research question: 'How can we translate our findings into practical and policy implications?' This includes measures focused on preventing cyber offending in the general population (primary prevention), activities targeted at relatively 'high-risk' groups (secondary prevention), and interventions directed at reducing recidivism for young people who are already involved in substantial levels of cyber-delinquency (tertiary prevention). This section is based on the results presented above and the suggestions put forward during the expert meeting. The experts at this meeting emphasised the importance of prevention and intervention efforts to address juvenile cyber-delinquency. Although several organisations in the Netherlands, such as the police and various municipalities, recently stressed the importance of interventions aimed at

prevention, they also indicated that they were still struggling as to how to prevent cyber-offenders from reoffending in the future.

The results from our study suggest that prevention and intervention measures could focus on specific high-risk groups, such as ICT students, who have relatively high rates of self-reported involvement in cyber-delinquency. For cyber-dependent crime, interventions could focus on individual factors such as computer addiction, self-control and (to a lesser extent) gaming, whereas interventions relating to cyber-enabled crime may also need to address environmental factors at home and in schools. However, the experts pointed out that it is not a matter of 'one size fits all' and emphasised that stereotypes about young cyber-offenders are often incorrect and that groups of offenders can differ. In addition, motivations and ICT skill levels may differ substantially between offenders. Interventions should be able, therefore, to examine the motives and needs of an offender and tailor the intervention to the individual.

While organisations such as the police and probation services play an important role in prevention, schools and parents may also be helpful in preventing cyber-offending early in an individual's criminal career. For schools, our results on environmental factors show that it may be helpful to increase school satisfaction in general. Our results do not indicate clear opportunities for school interventions directed specifically at cyber-offending. For example, online rules at school were not shown to have an effect. However, schools may be able to spot early signs of potential delinquency among their students and act on these signs. While school rules alone do not seem to have an effect, the effect of additional interventions at school that go beyond setting online rules could be examined in the future.

Additionally, the experts discussed that the link between positive and negative cyber-behaviour suggested that there was potential for schools to lead students away from negative behaviour, while also encouraging positive behaviour. A group of offenders would also appear to be interested in the prosocial side of cyber-behaviour. Additionally, schools could provide lessons on the distinction between 'good' and 'bad' cyber-behaviour and encourage their students to choose the positive alternative. Internships at, for example, ICT organisations or in a school's ICT department may provide older students with a clearer perspective on a future in which they can use their cyber-skills legally. As parents may not necessarily be aware of these internships and the opportunities for a career in ICT, schools can play an important role in providing such information. It should be noted, however, that the effect that these efforts

have on offending behaviour will need to be evaluated. But as our results showed an overlap between positive and negative cyber-behaviour, there is no guarantee that increasing positive behaviour will reduce negative behaviour.

Our results suggest that, in addition to schools, parents may play a role in preventing cyber-delinquency, especially cyber-enabled offences. Increasing online rules by parents and reducing time spent at home alone may reduce cyber-enabled delinquency. However, the experts suggested that parents may need some guidance on how to prevent children's online delinquency. Schools may also be able to involve parents in interventions aimed at prevention, for example by raising awareness among parents and offering them suggestions on making online rules and supervising their children's online behaviour.

Finally, with respect to peer offending, our results suggest that it may be less important to focus prevention and intervention measures on the direct influence of peers' *actual* behaviour or on trying to prevent an individual from becoming friends with cyber-delinquent individuals. This is also difficult, given that the online behaviour of friends may be less visible than offline behaviour. By contrast, prevention and intervention can be expected to benefit from addressing the extent to which individuals are influenced by the *perceived* cyber-delinquency of friends. In addition to targeting (perceptions about) school friends, our results suggest that it is very important for prevention and intervention measures also to target other types of friends (and perceptions about these friends), including online friends and real-life friends outside school.

All in all, our results suggest that prevention and intervention measures should address various factors together and should distinguish between specific groups of offenders and their needs. In addition to criminal justice organisations, such as the police and probation services, schools and parents may play an important role in preventing and reducing negative cyber-behaviour, but also in encouraging positive cyber-behaviour as opposed to cyber-offending.

References

Agnew, R. (1991). The interactive effect of peer variables on delinquency. *Criminology*, *29*(1), 47–72.

Akers, R. L. (1973). *Deviant Behavior: A Social Learning Approach*. Belmont, CA: Wadsworth, https://doi.org/10.1006/pest.1995.1007.

Akers, R. L. (1998). *Social learning and social structure: A general theory of crime and deviance*. Boston: Northeastern University Press.

Bae, S. M. (2017). The influence of strain factors, social control factors, self-control and computer use on adolescent cyber delinquency: Korean National Panel Study. *Children and Youth Services Review*, *78*, 74–80, https://doi.org/10.1016/j.childyouth.2017.05.008.

Baerveldt, C., Van Duijn, M. A. J., Vermeij, L., & Van Hemert, D. A. (2004). Ethnic boundaries and personal choice. Assessing the influence of individual inclinations to choose intra-ethnic relationships on pupils' networks. *Social Networks*, *26*(1), 55–74, https://doi.org/10.1016/j.socnet.2004.01.003.

Baerveldt, C., Völker, B., & Van Rossem, R. (2008). Revisiting Selection and Influence: An Inquiry into the Friendship Networks of High School Students and Their Association with Delinquency. *Canadian Journal of Criminology and Criminal Justice*, *50*(5), 559–587, https://doi.org/10.3138/cjccj.50.5.559.

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, https://doi.org/10.1007/s10940-015-9255-8.

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* (38–67), New York, https://doi.org/10.4018/978-1-61692-805-6.ch003.

Bruinsma, G. J. N., Pauwels, L. J., Weerman, F. M., & Bernasco, W. (2015). Situational action theory: Cross-sectional and cross-lagged tests of its core propositions. *Canadian journal of criminology and criminal justice*, *57*(3), 363–398.

Bunders, D., & Weerman, F. M. (2020). Social Media and Delinquency: Exploring the Relation between Online/Offline Interaction with Friends and Online/Offline Delinquency. *Kriminologie - Das Online-Journal*, (2), 283–309.

Burk, W. J., Kerr, M., & Stattin, H. (2008). The co-evolution of early adolescent friendship networks, school involvement, and delinquent behaviors. *Revue Francaise de Sociologie*, *49*(3), 499–522.

Burk, W. J., Steglich, C. E. G., & Snijders, T. A. B. (2007). Beyond dyadic interdependence: Actor-oriented models for co-evolving social networks and individual behaviors. *International Journal of Behavioral Development*, *31*(4), 397–404, https://doi.org/10.1177/0165025407077762.

Dahl, V., & Van Zalk, M. (2014). Peer networks and the development of illegal political behavior among adolescents. *Journal of Research on Adolescence*, *24*(2), 399–409, https://doi.org/10.1111/jora.12072.

Davis, J. A. (1970). Clustering and Hierarchy in Interpersonal Relations: Testing Two Graph Theoretical Models on 742 Sociomatrices. *American Sociological Review*, *35*(5), 843–851.

De la Rue, L. (2015). *The influence of family and friends on girls' delinquency: a social network analysis*.

Dijkstra, J. K., Berger, C., & Lindenberg, S. (2011). Do physical and relational aggression explain adolescents' friendship selection? The competing roles of network characteristics, gender, and social status. *Aggressive Behavior*, *37*(5), 417–429, https://doi.org/10.1002/ab.20402.

Farrington, D. P. (1986). Age and crime. *Crime and Justice*, *7*, 189-250.

Felson, M. (2003). The process of co-offending. In M. J. Smith & D. B. Cornish (Eds.), *Theory for Practice in Situational Crime Prevention (Vol. 16)* (pp. 149–168). Monsey, NY: Criminal Justice Press.

Field, A. (2013). *Discovering Statistics Using IBM SPSS Statistics - 4th edition*. London: SAGE Publications Ltd.

Flanagan, I. M., Auty, K. M., & Farrington, D. P. (2019). Parental supervision and later offending: A systematic review of longitudinal studies. *Aggression and violent behavior*, *47*, 215–229.

Gallupe, O., McLevey, J., & Brown, S. (2018). Selection and Influence: A Meta-Analysis of the Association Between Peer and Personal Offending. *Journal of Quantitative Criminology*, *35*(2), 313–335, https://doi.org/10.1007/s10940-018-9384-y.

Glueck, S., & Glueck, E. (1950). *Unraveling juvenile delinquency*. New York: Commonwealth Fund.

Goldsmith, A., & Brewer, R. (2015). Digital drift and the criminal interaction order. *Theoretical Criminology*, *19*(1), 112–130, https://doi.org/10.1177/1362480614538645.

Gordon, K. R. (2018). High School Students ' Perceptions of School Climate in Relation to Discipline History and Discipline Approach, 1–134, https://doi.org/https://scholarworks.umass.edu/dissertations_2/1240.

Gottfredson, M. R., & Hirschi, T. (1990). *A general theory of crime*. Stanford, CA: Stanford University Press.

Grabosky, P. (2001). Virtual criminality: old wine in new bottles. *Social & Legal Studies*, *10*(2), 243–249.

Grasmick, H. G., Tittle, C. R., Bursik, R. J., & Arneklev, B. J. (1993). Testing the general theory of crime. *Journal of Research in Crime and Delinquency*, *30*(1), 5–29.

H.M. Government. (2016). *National Cyber Security Strategy 2016-2021*. Consulted: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.

Haynie, D. L. (2001). Delinquent Peers Revisited: Does Network Structure Matter? *American Journal of Sociology*, *106*(4), 1013–1057, https://doi.org/10.1086/320298.

Haynie, D. L. (2002). Friendship Networks and Delinquency: The Relative Nature of Peer Delinquency. *Journal of Quantitative Criminology*, *18*(2), 99–134, https://doi.org/Article.

Haynie, D. L., Doogan, N. J., & Soller, B. (2014). Gender, friendship networks, and delinquency: A dynamic network approach. *Criminology*, *52*(4), 688–722, https://doi.org/10.1111/1745-9125.12052.

Haynie, D. L., & Osgood, D. W. (2005). Reconsidering Peers and Delinquency: How do Peers Matter? *Social Forces*, *84*(2), 1109–1130.

Hirschi, T. (1969). *Causes of delinquency. TA - TT -*. Berkeley SE: University of California Press.

Hoeben, E. M., Meldrum, R. C., Walker, D., & Young, J. T. N. (2016). The role of peer delinquency and unstructured socializing in explaining delinquency and substance use: A state-of-the-art review. *Journal of Criminal Justice*, *47*, 108–122, https://doi.org/10.1016/j.jcrimjus.2016.08.001.

Hoeben, E. M., & Weerman, F. M. (2016). Why is involvement in unstructured socializing related to adolescent delinquency? *Criminology*, *54*(2), 242–281, https://doi.org/10.1111/1745-9125.12105.

Holt, T. J. (2007). Subcultural evolution? Examining the influence of on- and off-line experiences on deviant subcultures. *Deviant Behavior*, *28*(2), 171–198, https://doi.org/10.1080/01639620601131065.

Holt, T. J. (2013). Examining the forces shaping cybercrime markets online. *Social Science Computer Review*, *31*(2), 165–177.

Holt, T. J., & Bossler, A. M. (2014). An Assessment of the Current State of Cybercrime Scholarship. *Deviant Behavior*, *35*(1), 20–40, https://doi.org/10.1080/01639625.2013.822209.

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, https://doi.org/10.1007/s12103-011-9117-3.

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, https://doi.org/10.1080/0735648X.2010.9721287.

Holt, T. J., & Kilger, M. (2012). Examining Willingness to Attack Critical Infrastructure Online and Offline. *Crime & Delinquency*, *58*(5), 798–822.

Hutchings, A. (2014). Crime from the keyboard: Organised cybercrime, co-offending, initiation and knowledge transmission. *Crime, Law and Social Change*, *62*(1), 1–20, https://doi.org/10.1007/s10611-014-9520-z.

Jaishankar, K. (2008). Space transition theory of cyber crimes. In F. Schmalleger & M. Pittaro (Eds.), *Crimes of the Internet* (283–301). Upper Saddle River: Prentice Hall.

Janssen, H. J., Weerman, F. M., & Eichelsheim, V. I. (2017). Parenting as a Protective Factor against Criminogenic Settings? Interaction Effects between Three Aspects of Parenting and Unstructured Socializing in Disordered Areas. *Journal of Research in Crime and Delinquency*, *54*(2), 181–207, https://doi.org/10.1177/0022427816664561.

Jose, R., Hipp, J. R., Butts, C. T., Wang, C., & Lakon, C. M. (2016). Network Structure, Influence, Selection, and Adolescent Delinquent Behavior: Unpacking a Dynamic Process. *Criminal Justice and Behavior*, *43*(2), 264–284, https://doi.org/10.1177/0093854815605524.

Kandel, D. B. (1978). Similarity in real-life adolescent friendship pairs. *Journal of Personality and Social Psychology*, *36*(3), 306–312, https://doi.org/10.1037/0022-3514.36.3.306.

Kandel, D. B. (1996). The parental and peer contexts of adolescent deviance an algebra of interpersonal influences. *Journal of Drug Issues*, *26*(2), 289–315.

Kerr, M., Van Zalk, M., & Stattin, H. (2012). Psychopathic traits moderate peer influence on adolescent delinquency. *Journal of Child Psychology and Psychiatry and Allied Disciplines*, *53*(8), 826–835, https://doi.org/10.1111/j.1469-7610.2011.02492.x.

Knecht, A., Snijders, T. A. B., Baerveldt, C., Steglich, C. E. G., & Raub, W. (2010). Friendship and delinquency: Selection and influence processes in early adolescence. *Social Development*, *19*(3), 494–514, https://doi.org/10.1111/j.1467-9507.2009.00564.x.

Kohler, U., & Kreuter, F. (2009). *Data analysis using stata*. College Station, TX: Stata Press.

Lazarsfeld, P. E., & Merton, R. K. (1954). Friendship as a social process: a substantive and methodological analysis. In M. Berger (Eds.), *Freedom and Control in Modern Society* (18–66). New York: Van Nostrand.

Lee, I. A., & Preacher, K. J. (2013). Calculation for the test of the difference between two dependent correlations with one variable in common. Consulted: http://quantpsy.org/corrtest/corrtest2.htm.

Lemmens, J. S., Valkenburg, P. M., & Gentile, D. A. (2015). The Internet Gaming Disorder Scale. *Psychological Assessment*, *27*(2), 567–582, https://doi.org/10.1037/pas0000062.

Lemmens, J. S., Valkenburg, P. M., & Peter, J. (2011). Psychosocial causes and consequences of pathological gaming. *Computers in Human Behavior*, *27*(1), 144–152, https://doi.org/10.1016/j.chb.2010.07.015.

Leukfeldt, E. R. (2017). *Research Agenda the Human Factor in Cybercrime and Cybersecurity*. The Hague: Eleven International Publishing. Consulted: https://www.thehaguesecuritydelta.com/media/com_hsd/report/141/document/Research-Agenda-The-Human-Factor-in-Cybercrime-and-Cybersecurity.pdf.

Leukfeldt, E. R., & Holt, T. J. (2020). *The Human Factor of Cybercrime*. (R. Leukfeldt & T. J. Holt, Eds.). New York: Routledge.

Logis, H. A., Rodkin, P. C., Gest, S. D., & Ahn, H. J. (2013). Popularity as an organizing factor of preadolescent friendship networks: Beyond prosocial and aggressive behavior. *Journal of Research on Adolescence*, *23*(3), 413–423, https://doi.org/10.1111/jora.12033.

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, https://doi.org/10.1080/01639625.2013.867721.

McFadden, D. (1977). *Quantitative methods for analyzing travel behavior of individuals: some recent developments.* Institute of Transportation Studies, University of California.

McGuire, M., & Dowling, S. (2013a). Chapter 1: Cyber-dependent crimes. In *Cyber crime: A review of the evidence* (1–34). Home Office, https://doi.org/10.1016/j.echo.2011.03.004.

McGuire, M., & Dowling, S. (2013b). Chapter 2: Cyber-enabled crimes - fraud and theft. In *Cyber crime: A review of the evidence*. Home Office, https://doi.org/10.1080/11356405.2016.1269500.

McPherson, M., Smith-Lovin, L., & Cook, J. M. (2001). Birds of a Feather: Homophily in Social Networks. *Annual Review of Sociology*, *27*, 415–444. Consulted: https://www.jstor.org/stable/2678628?pq-origsite=summon&seq=1#metadata_info_tab_contents.

Meldrum, R. C., & Clark, J. (2015). Adolescent virtual time spent socializing with Peers, Substance use, and Delinquency. *Crime and Delinquency*, *61*(8), 1104–1126, https://doi.org/10.1177/0011128713492499.

Miller, B., & Morris, R. G. (2016). Virtual Peer Effects in Social Learning Theory. *Crime and Delinquency*, *62*(12), 1543–1569, https://doi.org/10.1177/0011128714526499.

Molano, A., Jones, S. M., Brown, J. L., & Aber, J. L. (2013). Selection and socialization of aggressive and prosocial behavior: The moderating role of social-cognitive processes. *Journal of Research on Adolescence*, *23*(3), 424–436, https://doi.org/10.1111/jora.12034.

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* (1–17). New York: Information Science Reference.

Morris, R. G., & Blackburn, A. G. (2009). Cracking the Code: an Empirical Exploration of Social Learning Theory and Computer Crime. *Journal of Crime and Justice*, *32*(1), 1–34, https://doi.org/10.1080/0735648X.2009.9721260.

Nagin, S. D. (2013). Deterrence in the 21st Century: A Review of the Evidence. *Crime and Justice*, *42*(1), 199-263.

National Crime Agency. (2017). *Pathways into cyber crime*. Consulted: https://www.nationalcrimeagency.gov.uk/who-we-are/publications/6-pathways-into-cyber-crime-1/file.

ONS. (2020). Nature of crime: Fraud and computer misuse year ending March 2020 (dataset). Office for National Statistics. Consulted: https://www.ons.gov.uk/file?uri=/peoplepopulationandcommunity/crimeandjustice/datasets/natureofcrimefraudandcomputermisuse/yearendingmarch2020/natureofcrimefraudandcomputermisuse201920.xlsx.

ONS. (2021). *Crime in England and Wales: Year Ending September 2020*. *Office for National Statistics*. Consulted: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingseptember2020/pdf.

Osgood, D. W., & Anderson, A. L. (2004). Unstructured Socializing and Rates of Delinquency. *Criminology*, *42*(3), 519–550, https://doi.org/10.1111/j.1745-9125.2004.tb00528.x.

Osgood, D. W., Feinberg, M. E., & Ragan, D. T. (2015). Social Networks and the Diffusion of Adolescent Problem Behavior: Reliable Estimates of Selection and Influence from Sixth Through Ninth Grades. *Prevention Science*, *16*(6), 832–843, https://doi.org/10.1007/s11121-015-0558-7.

Pratt, T. C., Cullen, F. T., Sellers, C. S., Winfree, L. T., Madensen, T. D., Daigle, L. E., Fearn, N. E., Gau, J. M. (2010). The empirical status of social learning theory: A meta-analysis. *Justice Quarterly*, *27*(6), 765–802, https://doi.org/10.1080/07418820903379610.

Ripley, R. M., Snijders, T. A. B., & Preciado, P. (2020). *Manual for SIENA version 4.0*. Consulted: http://www.stats.ox.ac.uk/snijders/siena/.

Rogers, M. K. (2001). *A social learning theory and moral disengagement analysis of criminal computer behaviour: an explanatory study*. University of Manitoba.

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, https://doi.org/10.1177/1477370815617186.

Rokven, J. J., Weijters, G., & Van Der Laan, A. M. (2017). *Jeugddelinquentie in de virtuele wereld: Een nieuw type daders of nieuwe mogelijkheden voor traditionele daders?* The Hague.

Rulison, K. L., Gest, S. D., & Loken, E. (2013). Dynamic social networks and physical aggression: The moderating role of gender and social status among peers. *Journal of Research on Adolescence*, *23*(3), 437–449, https://doi.org/10.1111/jora.12044.

Shin, H. (2017). Friendship Dynamics of Adolescent Aggression, Prosocial Behavior, and Social Status: The Moderating Role of Gender. *Journal of Youth and Adolescence*, *46*(11), 2305–2320, https://doi.org/10.1007/s10964-017-0702-8.

Shrum, W., Cheek, N. H., & Hunter, S. M. (1988). Friendship in School : Gender and Racial Homophily. *Sociology of Education*, *61*(4), 227–239.
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.
Snijders, T. A. B. (2001). The statistical evaluation of social network dynamics. *Sociological Methodology*, *31*(1), 361–395. https://doi.org/10.1111/0081-1750.00099.
Snijders, T. A. B. (2020). RscriptMultipleGroups_meta.R: a script illustrating RSiena meta-analysis. Consulted: https://www.stats.ox.ac.uk/~snijders/siena/RscriptMultipleGroups_meta.R.
Snijders, T. A. B., Van de Bunt, G. G., & Steglich, C. E. G. (2010). Introduction to stochastic actor-based models for network dynamics. *Social Networks*, *32*(1), 44–60, https://doi.org/10.1016/j.socnet.2009.02.004.
Soudijn, M. R. J., & Zegers, B. C. H. T. (2012). Cybercrime and virtual offender convergence settings. *Trends in Organized Crime*, *15*(2–3), 111–129, https://doi.org/10.1007/s12117-012-9159-z.
Steglich, C. E. G., Snijders, T. A. B., & Pearson, M. (2010). Dynamic networks and behavior: separating selection from influence. *Sociological Methodology*, *40*(1), 329–393.
Steiger, J. H. (1980). Tests for comparing elements of a correlation matrix. *Psychological Bulletin*, *87*(2), 245–251, https://doi.org/10.1037/0033-2909.87.2.245.
Suler, J. (2004). The Online Disinhibition Effect. *CyberPsychology & Behavior*, *7*(3), 321–326. https://doi.org/10.1089/1094931041291295.
Sutherland, E. H. (1947). Principles of criminology. New York: JB Lippincott.
Svensson, Y., Burk, W. J., Stattin, H., & Kerr, M. (2012). Peer selection and influence of delinquent behavior of immigrant and nonimmigrant youths: Does context matter? *International Journal of Behavioral Development*, *36*(3), 178–185, https://doi.org/10.1177/0165025411434652.
Sweeten, G. (2012). Scaling criminal offending. *Journal of Quantitative Criminology*, *28*(3), 533–557.
Sweeten, G., Piquero, A. R., & Steinberg, L. (2013). Age and the explanation of crime, revisited. *Journal of youth and adolescence*, *42*(6), 921–938.
Turanovic, J. J., & Young, J. T. N. (2016). Violent Offending and Victimization in Adolescence: Social Network Mechanisms and Homophily. *Criminology*, *54*(3), 487–519, https://doi.org/10.1111/1745-9125.12112.
UCLA. (2011). What are pseudo R-squares? Consulted: 25 October 2020: https://stats.idre.ucla.edu/other/mult- pkg/faq/general/faq-what-are-pseudo-r-squareds/.
UK Home Office. (2018). Call for Multi-Year Research Proposals: “Understanding cyber offenders, criminal careers and business models”.
Van Der Laan, A. M., & Goudriaan, H. (2016). *Monitor jeugdcriminaliteit: Ontwikkelingen jeugdcriminaliteit 1997-2015*. The Hague.
Van der Toolen, Y., Weulen Kranenbarg, M., & Weerman, F. M. (2020). Online jeugdcriminaliteit en ‘verkeerde vrienden’: wanneer is de samenhang het sterkst?, *62*(2–3).
Van der Wagen, W., Van ’t Zand-Kurtovic, E. G., Matthijsse, S. R., & Fischer, T. F. C. (2019). *Cyberdaders: uniek profiel, unieke aanpak? Een onderzoek naar kenmerken van en passende interventies voor daders van cybercriminaliteit in enge zin*. The Hague.

Van Zalk, M. H. W., & Van Zalk, N. (2015). Violent peer influence: The roles of self-esteem and psychopathic traits. *Development and Psychopathology*, *27*(4), 1077–1088, https://doi.org/10.1017/S0954579415000693.
Veenstra, R., & Dijkstra, J. K. (2011). Transformations in Adolescent Peer Networks. In B. Laursen & W. A. Collins (Eds.), *Relationship Pathways: From Adolescence to Young Adulthood* (pp. 135–154), New York: Sage.
Viechtbauer, W. (2011). Conducting meta-analyses in R with the metafor package. *Journal of Statistical Software*, *36*(3), 1–48.
Walker, D. A. (2003). JMASM9: Converting Kendall's tau for correlational or meta-analytic analyses. *Journal of Modern Applied Statistical Methods*, *2*(2), 525–530, https://doi.org/10.22237/jmasm/1067646360.
Warr, M. (2002). *Companions in crime: the social aspects of criminal conduct*. Cambridge: Cambridge University Press. Consulted: http://catdir.loc.gov/catdir/samples/cam031/2001037395.html.
Wasserman, S., & Galaskiewicz, J. (1994). *Advances in social network analysis: Reseach in the social and behavioral sciences*. Thousand Oaks: Sage.
Weerman, F. M. (2010). Delinquency after secondary school: Exploring the consequences of schooling, working and dropout. *European Journal of Criminology*, *7*(5), 339–355.
Weerman, F. M. (2011). Delinquent peers in context: a longitudinal network analysis of selection and influence effects. *Criminology*, *49*(1), 253–286.
Weerman, F. M. (2020). Criminaliteit, digitalisering en de online sociale wereld: dezelfde processen in een nieuwe sociale context? *Tijdschrift voor Criminologie*, *61*(4).
Weerman, F. M., Bijleveld, C. C. J. H., & Averdijk, M. D. E. (2005). Netwerken en netwerkposities van delinquente en niet-delinquente jongeren. *Tijdschrift voor Criminologie*, *47*(1), 24–41.
Weerman, F. M., & Hoeve, M. (2012). Peers and delinquency among girls and boys: Are sex differences in delinquency explained by peer factors? *European Journal of Criminology*, *9*(3), 228–244.
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, https://doi.org/10.1111/j.0011-1348.2005.00015.x.
Weerman, F. M., Wilcox, P., & Sullivan, C. J. (2018). The Short-Term Dynamics of Peers and Delinquent Behavior: An Analysis of Bi-weekly Changes Within a High School Student Network. *Journal of Quantitative Criminology*, *34*(2), 431–463, https://doi.org/10.1007/s10940-017-9340-2.
Weulen Kranenbarg, M. (2018). *Cyber-offenders versus traditional offenders: An empirical comparison (Doctoral dissertation)*. Consulted: http://dare.ubvu.vu.nl/bitstream/handle/1871/55530/complete dissertation.pdf?sequence=6&isAllowed=y.
Weulen Kranenbarg, M., Holt, T. J., & Van Gelder, J. L. (2019). Offending and Victimization in the Digital Age: Comparing Correlates of Cybercrime and Traditional Offending-Only, Victimization-Only and the Victimization-Offending Overlap. *Deviant Behavior*, *40*(1), 40–55, https://doi.org/10.1080/01639625.2017.1411030.
Weulen Kranenbarg, M., Ruiter, S., & Van Gelder, J. L. (2021). Do cyber-birds flock together? Comparing deviance among social network members of cyber-dependent offenders and traditional offenders. *European Journal of Criminology, 18*(3), 386-406, https://doi.org/https://doi.org/10.1177/1477370819849677.

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

Zullig, K. J., Koopman, T. M., Patton, J. M., & Ubbes, V. A. (2010). School climate: Historical review, instrument development, and school assessment. *Journal of Psychoeducational Assessment*, *28*(2), 139–152, https://doi.org/10.1177/0734282909344205**.**

About the authors

Dr Marleen Weulen Kranenbarg (supervisor and project lead) is Assistant Professor in Criminology at the Vrije Universiteit (VU) Amsterdam and research fellow at the Netherlands Institute for the Study of Crime and Law Enforcement (NSCR). She conducts research focusing mainly on aspects of cyber-dependent offending and ethical hacking. Her PhD research entitled 'Cyber-offenders versus traditional offenders: an empirical comparison' was the first empirical comparison of cyber-dependent offenders with traditional offenders. Her comparison on the effect of social ties for cyber-offending and traditional offending resulted in the research questions answered in this report. Dr Weulen Kranenbarg is a member of the Steering Committee of the International Interdisciplinary Research Consortium on Cybercrime (IIRCC) and the Board of the European Society of Criminology (ESC) Working Group on Cybercrime.

Yaloe van der Toolen MSc (main researcher) is now in training to become a criminal investigator at the police. During the reseach for this report, she worked as a junior researcher at the Netherlands Institute for the Study of Crime and Law Enforcement (NSCR) and at the Vrije Universiteit (VU) Amsterdam. She has an academic background in Crime Science, Clinical Psychology and Political Science.

Prof. Frank Weerman (co-researcher and consultant) is a senior researcher at the Netherlands Institute for the Study of Crime and Law Enforcement (NSCR) and an Endowed Professor in Youth Criminology at the Erasmus University Rotterdam (EUR). Much of his research has focused on explaining traditional forms of juvenile delinquency, with a special focus on the role of peers. This includes the collection of self-reports and social network data in longitudinal survey designs. Other fields of interest are criminological theory, the role of schools and parents in youth delinquency, gangs and co-offending, radicalisation and terrorism.

Appendix: Details on individual and environmental items

Variable	Item(s) (translated from Dutch to English)	Answer options (translated from Dutch to English)
INDIVIDUAL CHARACTERISTICS VARIABLES		
Low self-control (composite of 9 items; alpha = 0.72)	I immediately say what I think, even though that's not always the smartest thing to do. When I feel like doing something, I immediately do it. I get angry easily. When I am truly angry, it is better for other people to stay out of my way. I am easily bored. I avoid things that I find hard to do. I often act without thinking about the consequences. Sometimes I take risks just for the fun of it. I'm good at patching up a quarrel (reverse).	Disagree completely; Disagree slightly; Do not disagree/Do not agree; Agree slightly; Agree completely; Don't know/Prefer not to say
Social skills (composite of 4 items; alpha = 0.78)	Starting a conversation with a stranger I find…; Showing my feelings to someone I find…; Introducing myself to someone I haven't met before I find…; Talking with someone about something I feel ashamed of I find…	Very difficult; Somewhat difficult; Not difficult / not easy; Somewhat easy; Very easy; Don't know/Prefer not to say
Computer addiction (composite of 6 items; alpha = 0.74)	In the past three months there have been periods during which all I could think of was the moment I could use the computer again (preoccupation). In the past three months I have been feeling unsatisfied because I wanted to use the	Never; Sometimes; Often; Don't know/Prefer not to say

	computer more often (tolerance). In the past three months I did not manage to reduce my computer time, whereas others had told me that I should use the computer less (persistence). In the past three months I used the computer so that I would not have to think about matters that distress me (escape). In the past three months I have had problems with others about the consequences of my computer behaviour (problems). In the past three months I have hidden the amount of time I am using the computer from others (deception).	
ICT knowledge	Which statement is most applicable to you?	0. I don't like using computers and don't use them unless I absolutely have to; 1. I can surf the net, use some common software but not fix my own computer; 2. I can use a variety of software and fix some computer problems I have; 3. I can use most software, and fix most computer problems I have; 4. I can use different programming languages and am capable of detecting programming errors
Gaming, average day	On the weekday just indicated by you, how many hours were you playing computer games, such as Fortnite, FIFA, League of Legends?	0 hours; 1-2 hours; 3-4 hours; 5-6 hours; 7-8 hours; More than 8 hours; Don't know/Prefer not to say
Positive cyber-behaviour (composite of 9 items; summation of dichotomised answers to separate behaviours)	How many times in the past 3 months... … have you actively participated in online forums on ICT topics such as programming, gaming or other computer technical topics? For example by posting messages, or by engaging in discussions. … have you shared self-developed codes or	Never; 1 time; 2 times; 3-5 times; 6-10 times; More than 10 times; Don't know/Prefer not to say

	software online with others? … have you taught others ICT? For example, teaching others how to program. … have you participated in ethical hacking events, such as hackathons? Ethical hacking means hacking to help people/companies, for example by testing security systems. … have you helped someone in your spare time with the design/editing of digital media? For example, making a movie, editing a photo, or designing a poster. … have you done ICT jobs on assignment? For example a job (on the side) or internship at an ICT company. … have you reported an ICT vulnerability (bug) via a bug bounty program? This program is used by companies/organisations to pay ethical hackers for finding an ICT vulnerability. … have you reported an ICT vulnerability via Coordinated Vulnerability Disclosure (CVD; also called Responsible Disclosure)? This allows you to share an ICT vulnerability with a company or organisation.	
ENVIRONMENTAL VARIABLES		
Offline rules by parents (composite of 4 items; alpha = 0.77)	My parents know where I am when I go somewhere in my spare time (e.g. at a friend's place). My parents know who I am with when I do something with others in my spare time. My parents know what I am doing when I go somewhere in my spare time (e.g. hanging around in the neighbourhood with friends).	Disagree completely; Disagree slightly; Do not disagree/Do not agree; Agree slightly; Agree completely; Don't know/Prefer not to say

	My parents have set clear rules about what I am allowed to do in my spare time.	
Online rules by parents (composite of 4 items; alpha = 0.82)	My parents know which websites and apps I use. My parents know who I talk to online and on social media. My parents know what I am doing when I am on my computer (e.g. gaming, social media, homework). My parents have set clear rules about my internet and computer use.	Disagree completely; Disagree slightly; Do not disagree/Do not agree; Agree slightly; Agree completely; Don't know/Prefer not to say
Home alone	On the weekday just indicated by you, how many hours were you at home alone without any parents/carers present?	0 hours; 1-2 hours; 3-4 hours; 5-6 hours; 7-8 hours; More than 8 hours; Don't know/Prefer not to say
Computer alone	On the weekday just indicated by you, how many hours were you using your computer/laptop WITHOUT adults knowing what you were doing on it?	0 hours; 1-2 hours; 3-4 hours; 5-6 hours; 7-8 hours; More than 8 hours; Don't know/Prefer not to say
Offline rules by school (composite of 4 items; alpha = 0.78)	My school has set clear rules on how you should and should not behave. My school puts a lot of effort into checking whether students stick to the rules (e.g. supervising teachers, CCTV cameras). If I do something that is not allowed, there's a good chance that I'll get caught. If I do something that is not allowed and I get caught, I am in big trouble.	Disagree completely; Disagree slightly; Do not disagree/Do not agree; Agree slightly; Agree completely; Don't know/Prefer not to say
Online rules by school (composite of 4 items; alpha = 0.80)	My school has clear rules about what you can and can't do on the computer (e.g. don't break into someone else's computer). My school puts a lot of effort into checking whether students follow the computer rules (e.g. checking what you do on the computer, keeping an eye on the network).	

	If I do something on the computer at school that's not allowed, there's a good chance I'll get caught. If I do something at school on the computer that's not allowed and I get caught, I am in big trouble.	
School satisfaction (composite of 4 items; alpha =.77)	I enjoy going to school. I feel at home at my school/on my education programme. I have a good relationship with the teachers from my school/on my education programme. I have a good relationship with the other students at my school/on my education programme.	Disagree completely; Disagree slightly; Do not disagree/Do not agree; Agree slightly; Agree completely; Don't know/Prefer not to say
School boredom	I feel bored when I am at school/my education programme.	Disagree completely; Disagree slightly; Do not disagree/Do not agree; Agree slightly; Agree completely; Don't know/Prefer not to say
ICT education satisfaction (composite of 2 items; alpha = 0.71)	The ICT classes at my school/education challenge me enough. I learn new things during my ICT classes.	Disagree completely; Disagree slightly; Do not disagree/Do not agree; Agree slightly; Agree completely; Don't know/Prefer not to say
Talk computer activities	My teachers discuss with me what I do on the computer at home.	Disagree completely; Disagree slightly; Do not disagree/Do not agree; Agree slightly; Agree completely; Don't know/Prefer not to say

For further information and communication about this report and study, contact Marleen Weulen Kranenbarg (corresponding author), email: M.WeulenKranenbarg@vu.nl.

Het NSCR is onderdeel van de institutenorganisatie van de Nederlandse Organisatie voor Wetenschappelijk Onderzoek (NWO)

Bezoekadres:
De Boelelaan 1077
1081 HV Amsterdam

Postadres:
Postbus 71304
1008 BH Amsterdam

T 020 598 5239
E nscr@nscr.nl
W www.nscr.nl

nscr

Nederlands Studiecentrum
Criminaliteit en Rechtshandhaving