This publication has been prepared on the occasion of the sixtieth anniversary of IPA Section the Netherlands, the Dutch branch of the International Police Association. It focuses on a range of studies centrally related to crime in a digitized society. The volume concentrates on policing and fighting crimes in a digital era. It provides several options and recommendations for implementing strategies that will allow the Dutch police to adapt to the quick changes in this field. The book provides an overall view of outcomes of recent cybercrime studies in the Netherlands and their implications for (inter)national police organisations. It is aimed primarily at the members of the IPA, but may also provide useful information for Police Academy students and police personnel who are involved in tackling cybercrime.

There is an increase of digital (ICT) components in traditional crimes. Hacking is now one of the top crimes in the Netherlands.The studies in this volume suggest that it is wise to enhance public private partnership, expand international collaboration and invest in police education. It is important to note that the digitization is never complete. The police is advised to closely examine and readjust their strategy where needed and take into account a change in police clientele. Although this volume provides some answers, new questions also emerge. More research is needed to grasp what is happening in this fast-changing digital world.

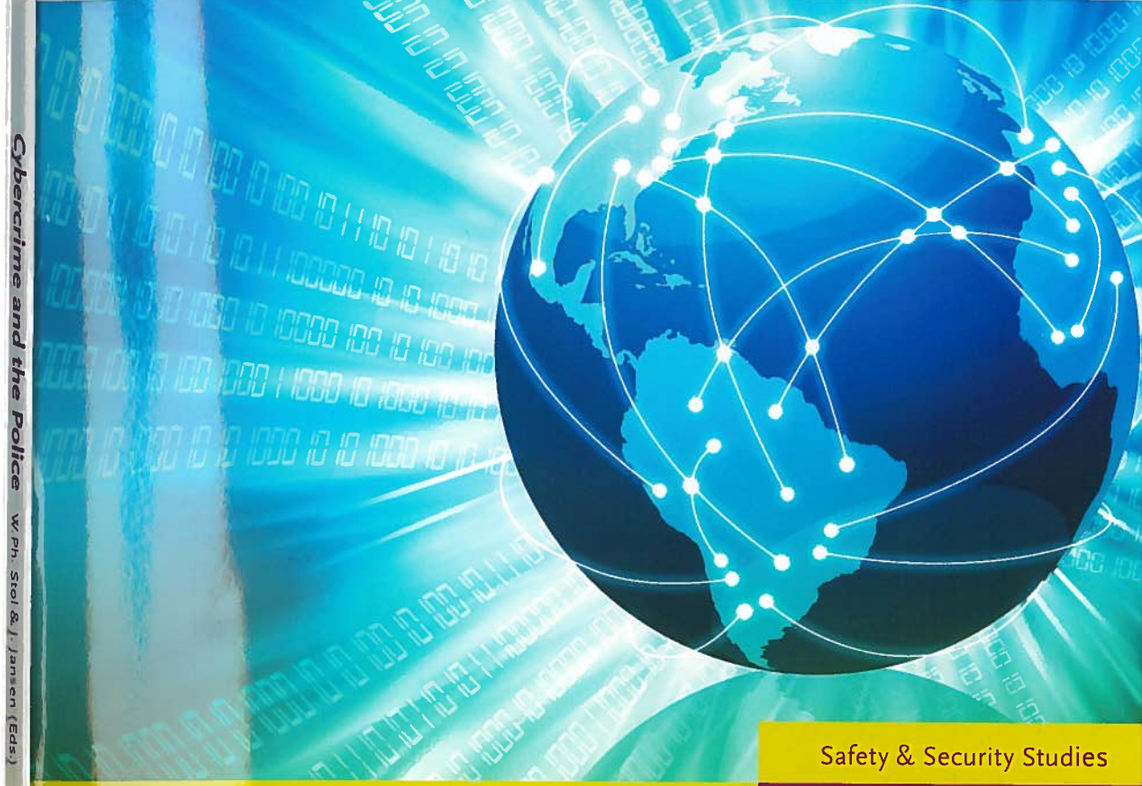
The IPA provides a large international network that is suitable for the exchange of knowledge, working methods and best practices. The Internet makes our world smaller and the playing field of criminals much larger. Cybercrime is a global phenomenon. This book contributes to the police profession on a topic that is of great importance.

The *Safety & Security Studies* series is an initiative of the network of Collaborating Institutions for Security (in Dutch: *Samenwerkende Kennisinstellingen voor Veiligheid*). The editors of the series are Evelien De Pauw MSc (Coordinator Research centre and lecturer in public safety and security, KATHO University College), Dr W.K.F. Rodenhuis (lector risk management at the Saxion University of Applied Sciences), Prof. Dr W.P. Stol (lector cyber safety at NHL University of Applied Sciences and the Police Academy of the Netherlands, professor police studies at the Open University) and Dr J. Timmer (lector security and social cohesion at Windesheim University of Applied Sciences).

INTERNATIONAL POLICE ASSOCIATION
ipa
WWW.IPA-NEDERLAND.NL

ISBN 978-94-6236-069-3

Cybercrime and the Police W.Ph. Stol & J. Jansen (Eds.)



Safety & Security Studies

Cybercrime and the Police

Edited by
W.Ph. Stol
J. Jansen

eleven
international publishing

Safety & Security Studies

The Safety & Security Studies are an initiative of the network of Collaborating Institutions for Security (in Dutch: *Samenwerkende Kennisinstellingen voor Veiligheid* (SKV network)) that comprises the Avans University of Applied Sciences, University of Applied Sciences Windesheim, The Hague University of Applied Sciences, Inholland University of Applied Sciences, Utrecht University of Applied Sciences, Zeeland University of Applied Sciences, Catholic University of South-west Flanders, Netherlands Institute for Physical Security *Nibra*, NHL University of Applied Sciences, Saxion University of Applied Sciences Enschede and the Police Academy of the Netherlands.

The editors of the series are Evelien De Pauw MSc (Coordinator Research centre and lecturer in public safety and security, KATHO University College), W.K.F. Rodenhuis MSc (lecturer risk management at the Saxion University of Applied Sciences), Prof. Dr W.Ph. Stol (lecturer cyber safety at NHL University of Applied Sciences and the Police Academy of the Netherlands, professor police studies at the Open University) and Dr J. Timmer (lecturer security and social cohesion at Windesheim University).

Previously published works in the Security Studies include:

- E.R. Leukfeldt, K.W.C. van der Straten, M.P. Kruis & W.Ph. Stol, *Ter plaatse. Alledaagse samenwerking tussen de primaire hulpdiensten* [On the spot. Everyday cooperation between primary care services] (2007)
- J. Kerstens, M. Toutenhoofd & W.Ph. Stol, *Wie niet weg is, is gezien. Gevalstudie over een proef met cameratoezicht in de Leeuwarder binnenstad* [In full view. Case study about an experiment using cameras in the center of Leeuwarden] (2008)
- W.Ph. Stol, H.W.K. Kaspersen, J. Kerstens, E.R. Leukfeldt & A.R. Lodder, *Filteren van kinderporno op internet. Een verkenning van technieken en reguleringen in binnen- en buitenland* [Filtering child pornography on the Internet. An exploration of techniques and regulations at home and abroad] (2008)
- L. Symons, J. Deklerck, D. Gelders & S. Pleysier, *Inbraakpreventief advies in België. De mening van de burger* [Advise about preventing break-ins in Belgium. The citizens' opinions] (2010)
- E.R. Leukfeldt, M.M.L. Domenie & W.Ph. Stol, *Verkenning cybercrime in Nederland 2009* [Investigating cybercrime in the Netherlands 2009] (2010)
- T. van Ham, E.R. Leukfeldt, B. Bremmers, W.Ph. Stol & A.Ph. van Wijk, *The art of the Internet. A study of illegal online trading in cultural goods* (2011)
- T. van Ham, E.R. Leukfeldt, B. Bremmers, W.Ph. Stol en A.Ph. van Wijk, *De kunst van het internet. Een onderzoek naar de online illegale handel in cultuurgoederen* (2011)
- J. Kerstens & W.Ph. Stol, *Jeugd en cybersafety. Online slachtoffer- en daderschap onder Nederlandse jongeren* [Youth and cybersafety: Online victimization and perpetration among Dutch Youth] (2012)
- M.M.L. Domenie, E.R. Leukfeldt, J.A. van Wilsem, J. Jansen & W.Ph. Stol, *Slachtofferschap in een gedigitaliseerde samenleving* [Victimization in a digitized society] (2013)

Cybercrime and the Police

Editors:

W.Ph. Stol

J. Jansen

eleven
international publishing

4 Offenders in a Digitized Society

Jurjen Jansen, Marianne Junger, Lorena Montoya and Pieter Hartel

4.1 Introduction

"In combatting cybercrime, with its borderless nature and huge ability for the criminals to hide, we need a flexible and adequate response." This quote from Troels Oerting (Head of the European Cybercrime Centre)[19] sets the tone for this chapter. In order to be able to respond flexibly and adequately to cybercrime, it is required to have insight into who commits these crimes. Therefore, this chapter focusses on perpetrators and what defines them.

First, results of the *Youth and Cybersafety Survey* among children aged 10–18 years are presented.[20] Second, the *Modus Operandi-Information Technology (MO-IT) Study* is presented. Both studies are described separately, in Sections 2 and 3, respectively.

Although both Dutch studies focus on offenders, and therefore are included in one and the same chapter, it should be noted that they also differ from each other. The two leading questions in the youth study are 'what percentage of youth commit cyber offences' (prevalence) and 'how offenders can be characterized' (sex, age, etc.). This information is important for the police since it clarifies the kind of persons they have to deal with in the case of digital crime. The first question in the MO-IT study is what percentage of fraud and threat can be labelled 'digital crime' (another way to define prevalence) and the second question is to what extent offenders of digital crimes differ from offenders of traditional crimes in terms of socio-demographic and socio-economic characteristics. In this sense, the MO-IT study goes one step further than the youth study, as it focusses on differences within offender populations and, consequently, whether the police have to adapt to a different clientele and/or a different work load.

Both studies do not provide us with all-embracing answers. They provide a picture of some groups of cyber offenders in the Dutch context. Still, the findings lead to conclusions that should be taken into account by those who are responsible for police policy with respect to cybercrime (see also Chapter 8).

19 Original source: <http://europa.eu/rapid/press-release_IP-13-13_en.htm>.

20 The first study was funded by the Dutch Ministry of Education, Culture and Science. The second study was funded by the Dutch National Police Agency and the Dutch police's Program Against Cybercrime.

4.2 Youth Offenders

When it comes to youth using the Internet, there is an immediate association with risks and victimization (*e.g.*, Chapter 3). However, youth can also engage in online deviant behaviour. For law enforcement agencies information about the prevalence of cyber offences and insight in the characteristics of offenders is essential in order to prevent, identify and investigate deviant online behaviour, especially when this behaviour can be considered criminal. Until recently, no comprehensive studies were available on online perpetration of children in the Netherlands. The primary goal of the *Youth and Cybersafety Survey*, a national survey on online perpetration (and victimization) among Dutch children aged 10–18 years, was to address this research gap.[21] First, the survey investigates the prevalence of online deviant/criminal behaviour among Dutch youth. Second, the survey identifies risk factors related to online perpetration. Three types of deviant/criminal behaviour are included: financial crimes (online auction fraud and virtual theft), cyberbullying and the production and distribution of sexual-oriented images and/or videos (posting sexy images on the Internet, making sexual images and/or videos of peers and stripping on a webcam). This section describes the research methods used to collect data, followed by an overview of the findings. The section ends with a discussion. At the end of this chapter, a table (Table 4) is presented that shows prevalence and background variables.

4.2.1 *Methods*[22]

The survey among Dutch youth (aged 10–18 years) was conducted between January 2011 and April 2011 in accordance with the Code of Conduct for Applied Research established by the HBO council (Andriessen, Onstenk, Delnooz, Smeijsters, & Peij, 2010). Parental consent and children's assent were obtained before participation. Parents were informed by a letter and were given the option to exclude their child from the survey. Participants were notified that the questionnaire would be about the Internet and online risks, that the investigators had no chance to identify who had given the answers and that they could terminate the survey at any point of time if they wished.

Data were collected using an online survey. The questionnaire was filled in at school during class. Primary and secondary schools were randomly sampled. Schools exclusively providing special or practical education were excluded from the sample, since children attending these schools require a different research approach. The response rate of schools was 15%. Ultimately, children from 27 primary schools and 17 secondary schools did participate. The response rate of children from the schools selected was 96.4% (N = 6,299). Statistical analysis showed that the sample did not deviate from national distributions of gender among Dutch children. However, it did deviate considering age; the age group 11–14 years is overrepresented. Of the participants, 29.3% were attending primary education (seventh and eighth grade) (n = 1,846) and 70.7% were attending secondary education (n = 4,453). For more information about the methods, see Kerstens and Stol (2012).

21 In the *Youth and cybersafety survey* both perpetration and victimization among youth were measured. Figures on online victimization are presented in Chapter 3.

22 This is an exact copy of the methods section in Chapter 3.

4.2.2 *Online Auction Fraud*

A small part of youth is engaged in online auction fraud. The respondents were asked whether they ever bought a product online, received it but never paid for it and whether they ever 'sold' a product, received money for it but never have sent the product to the 'buyer.' Respectively, 2.6% and 1.0% have done so. Of the surveyed youth, 3.1% can be considered perpetrator when both types of auction fraud are taken together. Statistical analyses show that boys are more involved with online auction fraud than girls. Furthermore, it is made clear that young people who commit online auction fraud have a beneath-average level of self-control. Finally, there is a strong relationship between victimization and perpetration: Those who commit online auction fraud are more likely to also be victim of this kind of fraud.

4.2.3 *Virtual Theft*

One in 10 (10.2%) has ever stolen virtual goods (*i.e.*, intangible objects in online games and virtual worlds,[23] which have a certain value and which can be bought and sold for real money in the offline world) from someone (see also Chapter 3). In all, 3.7% indicated that they have done this more than once. Offenders are predominantly male and in pre-vocational education. Children in primary school tend to be less often perpetrator of virtual theft. Certain Internet behaviour of children can be considered risk factors. Youth who spend more time online than average, who play games frequently, who give away personal information to others online and who undertake risky clicking behaviour (opening unknown e-mails, attachments and hyperlinks) are more prone being a perpetrator of virtual theft. Additionally, analyses indicate that there is some form of reciprocity between being a perpetrator and being a victim of virtual theft.

Finally, perpetrators are characterized by having low levels of self-control and show a higher level of psychosocial well-being. At first glance, this finding seems strange. A possible explanation is that the direction of the relationship is reversed: stealing virtual goods makes children happier instead of that happy children intend to steal. This assumption requires further explanation. Virtual theft eminently takes place within games and in those games where level or ranking systems are in place. The higher the level a player reaches, the more prestige, respect and appreciation that yields to the other players. In addition

23 For example, Habbo Hotel, World of Warcraft and RuneScape.

to such systems, there are also certain virtual goods that make an avatar (*i.e.*, an online character) stronger. When a young person has stolen an account with a high-level avatar or a very strong sword for his own avatar, then the appearance of this young person becomes higher. Perhaps, by means of stealing, the obtained higher status affects the psychosocial well-being of young people. Whether this assumption holds would require further research.

4.2.4 *Bullying*

Bullying is a form of aggression (see also Chapter 3). Although bullying is not a crime in itself, it can take on forms that are punishable. Respondents were asked questions about a range of online behaviours representing forms of cyberbullying, and, subsequently, the respondents were asked if they qualify their behaviour as bullying. Only when respondents confirmed their own behaviour as bullying were they considered perpetrators.

Of the surveyed youth, 3.8% admitted that in the past 3 months they are 'guilty' of gossiping, cursing/threatening, excluding, sending offensive pictures and/or videos and/or the placement of offensive pictures and/or videos on the Internet.[24] Statistical analyses show that the older youth (in secondary school) engage more often in cyberbullying than the younger ones (in primary school). An important finding is that cyberbullying is not an isolated phenomenon. Traditional bullying and cyberbullying are strongly intertwined: young people who bully at school and on the street also bully on the Internet and vice versa. Perpetrators are also more likely to be victims of offline bullying; so is the case with online bullying, but they react predominantly indifferently to this. Perpetrators of cyberbullying display Internet behaviour that deviates from the average; they are more often online and they behave online with less restraint than others (*i.e.*, online disinhibition).[25]

4.2.5 *Production and Distribution of Sexual-Oriented Images and/or Videos*

With all the technological possibilities of the Internet, smart phones and other devices with a camera, youth can relatively easily produce and disseminate sexually oriented photo and film material. This can range from undressing on a webcam to making sexual images and/or videos of each other and sharing these online with others. Making sexual imagery can be part of sexual experimentation. However, it is plausible that this material – without permission, for instance when a relationship is terminated – is placed online or will be used to

24 When discarding the self-evaluation the percentage of cyberbullies rises to 24.1%. This implies that the online bullying behaviour by the other 'perpetrators' is apparently not intentional.

25 The online disinhibition effect (Suler, 2004) represents the loosening (or complete abandonment) of social restrictions and inhibitions that would otherwise be present in normal face-to-face interaction during interactions with others on the Internet.

bully, extort or blackmail. Moreover, it is difficult to remove such material once it is placed online. In addition, this kind of sexual imagery can be considered child pornography. In the Netherlands, the possession, production and distribution of child pornography and viewing sexually explicit images of children younger than 18 years via a webcam is punishable according to Article 240b Sr.[26]

The respondents were asked whether in the past 6 months they have posted a 'sexy' picture of themselves on the Internet.[27] Of all youth, 3.1% has done so. Youth in pre-vocational education present themselves in this way more than youth within the higher educational levels. This behaviour is hardly visible among primary school children. Moreover, youth associated with this behaviour have a poor relationship with parents and display certain Internet behaviour (offenders visit social network sites more often, make compulsive use of Internet and give away personal information to others online). Finally, children who post sexy pictures of themselves on Internet have a beneath-average level of self-control.

Children in secondary school were also asked whether they have ever made sexual images and/or videos of their peers. The production and distribution of sexual images of others is quite rare (1.9%). In 59.0% of these cases, the material was for personal use only. In other cases, the material was sent to others (21.7%), distributed on the Internet (13.3%) and printed and distributed in the school (12.0%). Apart from these, 9.1% gave another answer. Most of these consider showing the pictures and/or videos to a friend or small group of friends. 'Offenders' are predominantly in senior general secondary school and of immigrant origin. Youth engaged in this behaviour is furthermore characterized by having a poor relationship with parents and having a low level of self-control.

The final form of making and distributing sexual images and/or videos is by the means of stripping on a webcam. Of all secondary school children, 1.6% has ever stripped on a webcam. This is mainly done by youth from non-traditional families, who have a poor relationship with their parent(s), who give away personal information to others online and who behave online with less restraint than others (*i.e.*, online disinhibition).

4.2.6 *Discussion*

Of all surveyed youth, 16.9% engaged in one or more forms of deviant online behaviour. Single perpetration is more common (13.7%) than multiple perpetrations (3.2%). The term perpetration and/or offender must be interpreted carefully because not all forms of deviant behaviour are punishable. Table 1 shows the prevalence of the individual offences presented in this section.

26 Children who have not reached the age of 12 cannot be punished under Dutch criminal law.

27 The word 'sexy' was chosen because the pre-test of the questionnaire revealed that this word by virtually all young people was unambiguously interpreted; as posing in (partly) exposed and provocative ways.

Table 1. Offenders of Deviant Online Behaviour

Deviant Behaviour	Prevalence (% Youth)
Virtual theft (ever)	10.2
Online auction fraud (ever)	3.1
Making sexual images and/or videos of peers (ever)	1.9
Stripping on a webcam (ever)	1.6
Posting sexy images on the Internet (past 6 months)	3.1
Cyberbullying (past 3 months)	3.8

Not only are young people culprit in the offline world, but they also demonstrate deviant behaviour on the Internet. However, online perpetration is less common than online victimization (see Chapter 3). The risk factors for deviant behaviour of youth on the Internet are diverse. Two factors that play an important part considering perpetration are giving away personal information to others online and behaving with less restraint on the Internet (*i.e.*, online disinhibition). For financial crimes, it is clear that most perpetrators are boys and that there is a reciprocal relationship between perpetration and victimization. The latter also counts for cyberbullying. Both being bullied and to bully and online and offline bullying behaviour are intertwined. One factor that stands out considering sexual 'deviant' behaviour is perpetrators having a poor relationship with their parents.

The main factor considering perpetration (except for bullying and stripping), however, is a low degree of self-control. These are young people who act impulsively, without thinking about possible consequences. According to Gottfredson and Hirschi (1990), the basis for self-control is laid during socialization processes in childhood (until about 8 years) and remains fairly stable throughout life. Self-control seems to be difficult to influence. Recent neurological research has demonstrated that the brains of young people function differently than those of adults in decision making (van Leijenhorst, 2010). Young people are more sensitive to the prospect of a possible reward and therefore more likely to take risks: They are looking for instant gratification. This would mean that low self-control not only is a predictor for online perpetration, but can also be considered as a general feature of the adolescent brain. Based on the survey results, it would seem sensible to try to teach young people to first think before impulsively responding to all kinds of (online) situations. However, considering the above, it is questionable whether this is feasible. It is recommended to conduct experiments in this area and evaluate if such things work. In addition, schools can focus on digital social rules, so that children gain more insight into the possible consequences of their online (deviant) behaviour.

Conclusively, an important question is whether youth is aware of the potential impact of online deviant behaviour that can be considered criminal, for example, making and distributing sexual images of minors (*i.e.*, child pornography) and virtual theft (which is – by law – the same as 'offline' theft). Qualitative

research on this topic (*e.g.*, van Dijk, van de Walle, Veenstra, Jansen, & Kerstens, 2012) shows that children – and also parents – are unaware of the criminalization of this kind of behaviour. This calls for awareness programmes. Law enforcement agencies also have an important role considering youth, especially when it involves sexual deviant behaviour. In the Netherlands, almost a quarter of the suspects in child pornography cases are younger than 24 years and 35% of that group is under 18 (Leukfeldt, Domenie, & Stol, 2010). If a young person is arrested and prosecuted under Article 240 Sr, it is implied that his or her judicial data are to be destroyed after 80 years. This means it can seriously hinder one's further life, for example, when applying for certain jobs which involves working with children. A complaint against a minor under Article 240 Sr may lead, even though the case was dropped, to a lifelong labelling. Thus, legislation designed to protect minors from sexual abuse also could prove particularly costly for minors who experiment with their sexuality over the Internet. The legislation thus appears not to take into account sexual experimental behaviour of teenagers. Perhaps legislation could be modified, but most certainly at least law enforcement needs to acknowledge this dilemma and take into account the far-reaching consequences that the prosecution of juveniles may have under these articles.

4.3 Offenders of Digital and Traditional Crimes

Do the new crime opportunities created by information and communication technologies (ICT) influence the type offenders that get involved in crime? Based on the Routine Activities approach (Felson, 2006; Felson & Clarke, 1998), this seems a plausible hypothesis. Opportunities for crime are created by the immediate environment and technology; new technologies shape new opportunities, and these developments can affect the type of offenders that get involved in crime (Felson, 2006; Felson & Clarke, 1998). Gould (1969), for instance, found that the increase in the number of automobiles after World War II led to a huge increase in car theft. This increase in car theft affected the population of offenders, and car thieves became increasingly younger.

Within this line of reasoning, it seems plausible that the introduction of ICT will affect crime and possibly also change the type of offenders. Several studies showed that there are differences in Internet use with respect to sex, age, socio-economic status and educational level (Banerjee, Kang, Bagchi-Sen, & Rao, 2005; van Deursen & van Dijk, 2012; Norris, 2001). For instance, women tend to use the Internet more often for shopping and for communication. Persons with a high educational level and high income tend to be more online and have more ICT devices than those with lower educational levels and lower income (van Deursen & van Dijk, 2012; Norris, 2001). These findings imply that different segments of the population have varying opportunities for cybercrime.

The introduction of ICT does probably not affect all types of crime equally. For instance, a previous study found that 16% of the threats and 41% of all frauds have – in part – a digital modus operandi, that is, the offenders made use of ICT

in the commission of the crime; to commit burglaries, offenders hardly ever use ICT (Junger, Montoya, & Hartel, 2013).

The MO-IT study investigated whether the growing presence of ICT technology influenced the type of offenders of threats and fraud. Two hundred and fifty-nine threats and two hundred and seventy-four cases of fraud that were reported to the police were analyzed.

4.3.1 Methods

The aim of the study was to collect information on 300 randomly selected cases of both threats and fraud that were registered by the police in the Eastern region of the Netherlands, in the provinces of Overijssel and Gelderland. To this end, for each crime, the determined numbers of cases were drawn randomly from all cases that were registered by the police and that took place in 2011. Data collection took place from March until June 2012.

To describe the crimes, a checklist was developed. Trained coders filled in a paper checklist at the police station and coded information from a printed version of the electronic file.[28] The following measures were used. *Threats* consist of various sorts of threats, including stalking, kidnapping/abduction and other offences against personal freedom. *Fraud* includes all sorts of fraud, including scams, counterfeiting of money or documents such as passports, identity cards, bank cards, ATM cards, checks, licenses, the possession of these false documents, and other types of fraud such as benefit fraud, insurance fraud, false declarations and bank fraud.

To determine whether a crime was 'digital', it was examined whether the crime was performed on the Internet, whether offenders threatened to disclose digital information, and whether emails were sent or whether other means of digital communication, such as text messages, were used to commit the crime. Coders had to read carefully the entire police file as this was not something that was registered in a standardized way by the Dutch police. If at least one digital modus operandi was used, the crime was considered 'digital.'

Information was collected on the following concepts. *Sex* was coded as male/female, it should be noted that in some cases, the offender was a business. *Age* was coded as younger or older than 35 years of age. *Nationality* was defined as country of birth. A distinction was made between born in the Netherlands or elsewhere. *Being employed* was coded as having – or not having – a legal occupation. *Criminal record* was coded as present or absent. The *number of offenders* that were involved in a case was coded as alone or more than one offender. The *relationship between offender and victim* consisted of different categories: a professional relationship, family, acquaintances, neighbours, ex-partners, partners, criminal contacts, online social network, fellow gamers, chat friends or another relationship. *Location* was coded in global terms: whether the victim and the

28 A copy of the checklist can be obtained from M. Junger (M.Junger@UTwente.nl).

offender were – at the moment of committing the crime – (a) both present in the Eastern Netherlands, (b) either the offender or the victim was present in the Eastern region, the other was elsewhere in the Netherlands, (c) either the offender or the victim was abroad, and (d) either the offender or the victim was outside the Eastern region. Finally, for each case, the coders filled in a brief description of the crime.

Seventy cases were double coded to assess inter-rater reliability. Overall, Kappa showed a good reliability (Junger et al., 2013).

The data were analyzed by computing contingency tables and chi squares. Besides looking at statistical significance of the chi squares, the size of the relationships was also evaluated. Several authors warned against relying exclusively on statistical significance testing and argued in favour of investigating the size of relationships when analyzing data (Carver, 1978; Schmidt, 1996). Therefore, odds ratios (ORs)[29] were computed in order to judge the size of the relationship between variables. Ninety-five per cent confidence intervals of the OR are also presented. A 95% confidence interval means that 95% of the observed confidence intervals will hold the true value of the OR. When a confidence interval includes 1, obviously, the relationship might be non-existent.

On many socio-demographic characteristics, there were relatively high numbers of missing values. In order not to miss information, all available cases were used.

4.3.2 Results

Information was collected on 259 threats and 274 cases of fraud. These cases involved 562 suspects (threats = 322; fraud = 240). Information was available for only parts of these suspects, and the numbers differed for the various items that were coded. Not all selected cases could be coded. There were several reasons for this. Some cases appeared to consist of a different crime than a threat or fraud, some cases had been registered in a different police force and therefore no information was available and some cases had been taken over by a different police force and again no information could be coded. Digital threats involved a wide variety of conflicts and problems in the relational sphere where the offender sent threats to the victim – in part – via ICT. The cases of digital fraud include two broad categories. First, online auction fraud, meaning generally that someone purchased goods on the Internet that were not delivered or, vice versa, that goods were delivered but not paid for. The second category is online banking fraud: the victim found out that money is missing from his/her bank account.

29 The odds ratio is a measure of effect size, describing the strength of association between two variables. An odds ratio of 1 indicates that the condition or event under study is equally likely to occur in both groups. An odds ratio greater than 1 indicates that the condition or event is more likely to occur in the first group. And an odds ratio less than 1 indicates that the condition or event is less likely to occur in the first group.

There are several differences between digital and traditional offenders when taking into account statistical significance (Table 2). Offenders of digital threats, aged 18 years or older, have a legal occupation (40.7%) more often than the same offenders of traditional threats (17.4%). The ORs suggest that there are additional trends as well. Offenders of digital threats are more often female (*OR* = 1.7), older (*OR* = 1.4), less often have a criminal record (*OR* = 0.5), and they more often acted alone (*OR* = 0.4) than offenders of traditional threats.

Table 2. Characteristics of Offenders of Digital and Traditional Crime, in % and OR

	Threats						Fraud					
	Traditional	Digital	Difference	Odds Ratio	Confidence Intervals (Lower	Higher)	Traditional	Digital	Difference	Odds Ratio	Confidence Intervals (Lower	Higher)
Sex, type of offender												
Females[b]	12.7	20.0	−7.3	1.7	(0.7	−4.1)	17.3	15.8	1.5	1.0	(0.4	−2.4)
Businesses	—	—	—	—	—	—	8.3	17.5	−9.2	—	—	—
Age, % below 35 of age	52.9	44.4	8.5	1.4	(0.6	−3.2)	47.3	61.5	−14.2	0.6	(0.2	−1.4)
Born in the Netherlands	79.9	81.5	−1.6	0.9	(0.3	−2.5)	71.6	96.0**	−24.4	0.1	(0.01	−0.8)
Job, occupation												
All offenders	14.0	25.0[a]	−11	2.0	(0.9	−4.5)	11.8	6.3	5.5	0.5	(0.2	−1.2)
Offenders 18 years of age and older	17.4	40.7**	−23.3	3.2	(1.4	−7.7)	16.2	26.9	−10.7	1.9	(0.7	−5.5)
Criminal record	30.1	18.2	11.9	0.5	(0.2	−1.2)	8.8	11.7	−2.9	1.4	(0.6	−3.0)
Only one offender	80.7	90.5	−9.8	0.4	(0.1	−1.3)	78.5	94.5**	−16.1	0.2	(0.7	−0.6)

[a] $p = 0.066$.
[b] Odds ratio for males and females.
** $p < 0.01$.

Offenders of digital fraud are more often born in the Netherlands (96.0%) than traditional offenders (71.6%). They also acted alone more often (94.5% vs. 78.5% for digital and traditional offenders, respectively). Again, the ORs suggest additional trends. Offenders of digital fraud are younger (OR = 0.6), have a legal occupation (OR = 1.9) and they have a criminal record (OR = 1.4) more often than offenders of traditional fraud.

Digital offenders and traditional offenders differ with respect to the relationship with their victims. Offenders of digital threats threaten their ex-partner more often (28.9%) than the offenders of traditional threats (15.5%) ($p < 0.05$). Digital fraud occurs relatively frequently between business partners (47.3% vs. 24% for digital and traditional fraud, respectively; $p < 0.05$) and occurs less often among acquaintances (1.8% vs. 7.0% for digital and traditional fraud, respectively; $p < 0.05$).

Most threats occur between persons that are both in the Eastern region at the moment of the crime. In the case of fraud, digitization is related to increasing geographical distance between victims and offenders: 64% of the digital cases of fraud, but only 19.4% of traditional fraud occurs while either the victim or the offender was not is the Eastern region but somewhere else in the Netherlands (Table 3). The number of international crimes remains small. In both types of fraud, the number of international cases is low; 13.9% of the digital cases and 12.3% of the traditional cases of fraud have an international character.

Table 3. Geographical Distance Between the Offender and the Victim for Traditional and Digital Crimes, at the Time of the Crime, in %

	Threats		Fraud**	
	Traditional	Digital	Traditional	Digital
Both were in Eastern region	88.1	80.6	57.5	19.4
Either the victim or the offender were in Eastern region, the other elsewhere in the Netherlands	7.9	19.4	27.4	63.9
International (either the offender or the victim were abroad)	1.7	—	12.3	13.9
Both were outside Eastern region	2.3	—	2.7	2.8
N	177	31	73	36

** $p < 0.01$.

4.3.3 *Discussion*

The MO-IT study compared offenders of digital threats and fraud with offenders of traditional threats and fraud.

In comparison with traditional offenders, offenders of digital *threats* are more often female, older and they do not have a criminal record of threats. In a previous study, Wachs and Wolf (2011) also reported that sex differences decrease in the digital world and that males and females have a more equal

share in threats than in the offline world. These results seem to suggest the hypothesis that digitization seems to 'normalize' offenders of threats, meaning that they differ less from the overall population than traditional offenders in the police registration do.

Furthermore, digital offenders of *threats* are more often employed and commit their crime more often alone than traditional offenders. There is a similar trend for fraud. Regarding the other characteristics, digital offenders of threats differ from digital offenders of fraud.

In comparison with traditional offenders, digital offenders of *fraud* are relatively young, more often born in the Netherlands, more often have a job, execute their crime more often alone and they have a criminal record slightly more often. They do not differ with respect to sex. The finding that digital offenders more often have a job, are born in the Netherlands and work alone would support the hypothesis of the 'normalization' of fraud, in line with the findings for threats.

The MO-IT findings are to some extent similar to previous findings. Leukfeldt and Stol (2011) also reported that digital and traditional offenders of fraud do not differ with respect to sex. In contrast with the MO-IT study, Leukfeldt and Stol (2011) reported that traditional offenders of fraud – and not digital offenders – more often have a job. Furthermore, they did not find any difference with respect to criminal record between digital and traditional offenders. Unlike the MO-IT study, Leukfeldt and Stol (2011) emphasize the similarity between digital and traditional fraudsters with the exception of age: They found that digital offenders of fraud are significantly younger than traditional offenders of fraud.

The differences between both studies can be the result of differences in methodology. For instance, the MO-IT sample consisted of cases registered by the police in Overijssel while Leukfeldt and Stol draw a sample from cases registered by the police in Zuid-Holland-Zuid, which is a more urbanized part of the country.[30] It is also possible that the differences are the result of historic developments in the Internet world and its criminals. Leukfeldt and Stol (2011) used somewhat older data, namely, data from 2005 to 2009, while the MO-IT study used data from 2011. The penetration of the Internet in everyday life keeps increasing. For instance, between 2005 and 2011, the proportion of people who use the Internet for banking increased from 50% to 79% (Akkermans, 2012).

The MO-IT results also show a clear geographical trend: The distance between offenders and victims increases for digital crimes. The fact that ICT permits a greater distance between the offender and the victim is plausible. Despite this increasing distance, international crimes are relatively rare. The fact that there is still only little international digital crime is remarkable. Articles in newspapers suggest that much digital crime is committed by offenders in other countries that are therefore somehow immune for a local criminal

30 The population density in Overijssel is appr. 340 inhabitants/km² and in Zuid-Holland 1,240 inhabitants/km² (source: <www.overijssel.nl> and <www.zuid-holland.nl>).

justice authority (Barham, 2013). The present findings do not confirm this. This is in line with earlier results. Leukfeldt et al. (2010) found, on the basis of police files, that in 14.5% of the cases the offender of an e-fraud acted from abroad. Furthermore, in a recent victim survey (see Chapter 3), Domenie, Leukfeldt, Van Wilsem, Jansen and Stol found that 19.2% of the victims of e-fraud reported that the perpetrator acted from abroad. In conclusion, it seems that, in spite of the borderless character of the Internet, in more than 80% of all e-frauds in the Netherlands the perpetrator acts from within the country. A possible explanation is that it remains difficult for offenders, due to cultural and language differences, to commit international crimes.

Several limitations of the MO-IT study should be acknowledged. The sample consists of cases reported to the police in Eastern region. The results can therefore not be extrapolated to the Netherlands as a whole. Only two types of crime were investigated, namely, fraud and threat. The information is based on victim reports as registered by the police, and it is not fully known how accurate these are. However, based on our reading of the files (Junger et al., 2013), it can be concluded that the police does not accurately register digital modus operandi. This could imply that the figures of digital crime might actually be higher. The present study should be replicated to investigate if the differences that were found between digital and traditional offenders are confirmed. A second limitation is that the findings are analyzed – partly – using effect sizes, not taking statistical significance into account. The exploratory nature of the present study, in our view, justified this line of reasoning. Further research needs to investigate whether the present results can be replicated.

Despite these limitations, the benefit of the present study is that it compared digital and traditional offenders for two types of crime. Few studies until now have presented a systematic comparison of these two types of offenders.

References

Akkermans, M. (2012). Nederland in Europese top met internetbankieren [The Netherlands in the European top considering Internet banking]. *Webmagazine*. Retrieved from <www.cbs.nl/nl-NL/menu/themas/vrije-tijd-cultuur/publicaties/artikelen/archief/2011/2011-3537-wm.htm>.

Andriessen, D., Onstenk, J., Delnooz, P., Smeijsters, H., & Peij, S. (2010). *Gedragscode praktijkgericht onderzoek voor het hbo; Gedragscode voor het voorbereiden en uitvoeren van praktijkgericht onderzoek binnen het Hoger Beroepsonderwijs in Nederland* [Code of conduct for applied research at HBO: Code of conduct for preparing and conducting applied research in higher vocation education in the Netherlands]. Delft, Netherlands: Elan Strategie & Creatie.

Banerjee, S., Kang, H., Bagchi-Sen, S., & Rao, H. (2005). Gender divide in the use of Internet applications. *International Journal of E-Business Research (IJEBR), 1*, 24–39. doi: 10.4018/jebr.2005040102.

Barham, J. (2013). International: Cybercrime. Russia's cybercrime haven. *Security Management*. Retrieved from <www.securitymanagement.com/article/russias-cybercrime-haven-004818>.

Carver, R. P. (1978). The case against statistical significance testing. *Harvard Educational Review, 48*, 378–399.

van Deursen, A., & J. van Dijk. (2012). *Trendrapport internetgebruik 2012: Een Nederlands en Europees perspectief* [Trend report Internet usage 2012: A Dutch and European perspective]. Enschede, Netherlands: Unversiteit Twente.

van Dijk, T., van de Walle, R., Veenstra, S., Jansen, J., & Kerstens, J. (2012). *Jeugd en cybersafety: Een kwalitatief onderzoek naar online risico's vanuit het perspectief van jongeren* [Youth and cybersafety: A quantitative study on online risks from the perspective of youth]. Leeuwarden, Netherlands: Lectoraat Cybersafety.

Domenie, M. M. L., Leukfeldt, E. R., Wilsem, J. A., Jansen, J., & Stol, W. Ph. (2013). *Slachtofferschap in een gedigitaliseerde samenleving: Een onderzoek onder burgers naar e-fraude, hacken en andere veelvoorkomende criminaliteit* [Victimization in a digital society: A survey among members of the public into e-fraud, hacking and other frequently occurring crimes]. The Hague, Netherlands: Boom Lemma uitgevers.

Felson, M. (2006). *Crime and nature*. Thousand Oaks, CA, USA: Pine Forge Press.

Felson, M., & Clarke, R. V. (1998). Opportunity makes the thief practical theory for crime prevention. In B. Webb (Ed.), *Police research series* (pp. 36). London, UK: Home Office.

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

Gould, L. (1969). The changing structure of property crime in an affluent society. *Social Forces, 48*, 50–59.

Junger, M., Montoya, L., & Hartel, P. (2013). *Modus Operandi onderzoek naar door Informatie en Communicatie Technologie (ICT) gefaciliteerde criminaliteit* [Modus Operandi research on by Information and Communication Technology (ICT) facilitated crime]. Enschede, Netherlands: Universiteit Twente.

Kerstens, J. & Stol, W. Ph. (2012). *Jeugd en cybersafety: Online slachtoffer- en daderschap onder Nederlandse jongeren* [Youth and cyber safety: Online victimization and perpetration among Dutch youth]. The Hague, Netherlands: Boom Lemma uitgevers.

van Leijenhorst, L. (2010). *Why teens take risks: A neurocognitive analysis of developmental changes and individual differences in decision-making under risk* (Thesis presented at Leiden University). Enschede, Netherlands: Print Partners Ipskamp B.V.

Leukfeldt, E. R., Domenie, M., & Stol, W. Ph. (2010). *Verkenning cybercrime in Nederland 2009* [Cybercrime in the Netherlands 2009]. The Hague, Netherlands: Boom Juridische uitgevers.

Leukfeldt, E. R., & Stol, W. Ph. (2011). De marktplaatsfraudeur ontmaskerd: Internetfraudeurs vergeleken met klassieke fraudeurs [The marketplace-fraudster exposed: Internet fraudsters compared with classical fraudsters]. *Secondant, 25*(6), 26–31.

Norris, P. (2001). *Digital divide: Civic engagement, information poverty, and the Internet worldwide*. Cambridge, UK: Cambridge University Press.

Schmidt, F. L. (1996). Statistical significance testing and cumulative knowledge in psychology: Implications for training of researchers. *Psychological Methods, 1*, 115–129. doi:10.1037/1082-989X.1.2.115.

Suler, J. R. (2004). The online disinhibition effect. *Cyber Psychology and Behavior, 7*, 321–326.

Wachs, S., & Wolf, K. D. (2011). Correlates of cyberbullying and bullying – First results of a self-report study. *Prax kinderpsychologie kinderpsychiatrie, 60*, 735–744.

Table 4. Prevalence of Perpetration (Youth and Cyber Safety Survey) (in %)

Background Variables	Auction Fraud	Virtual Theft	Cyber-bullying	Posting Sexy Images on the Internet	Making Sexual Images and/or Videos of Peers	Stripping on a Webcam
Sex	**	**			**	
Male	4.5	15.8	4.0	2.7	2.6	1.7
Female	1.6	4.4	3.6	3.5	1.2	1.4
Age	**	**	**	**	*	**
(8–)10	1.3	3.3	1.1	0.9		
11–12	2.2	7.7	2.9	1.6	1.0	0.8
13–14	3.8	12.8	4.3	4.2	1.7	1.3
15–16	4.3	12.3	5.7	4.2	2.5	2.5
17+	3.2	12.7	4.8	6.0	4.0	2.8
School type	**	**	**	**		
Primary school	1.5	5.3	2.3	0.9		
Secondary school	3.8	12.2	4.4	4.1		
Educational level	**		**	**	**	
VMBO (pre-vocational education)	4.8	13.2	6.2	5.5	1.6	1.3
HAVO (senior general secondary education)	3.1	12.9	3.9	4.0	3.0	2.3
VWO (pre-university education)	2.9	10.6	2.8	2.4	1.5	1.3
Total	3.1	10.2	3.8	3.1	1.9	1.6

*$p < 0.05$. **$p < 0.01$.