How 'Digital' is Traditional Crime?

Lorena Montoya*, Marianne Junger† Pieter Hartel*,
*Distributed and Embedded Security Group
†Industrial Engineering and Business Information Systems
University of Twente, The Netherlands
{a.l.montoya, pieter.hartel, m.junger}@utwente.nl

***Abstract*—Measuring how much cybercrime exists is typically done by first defining cybercrime and then quantifying how many cases fit that definition. The drawback is that definitions vary across countries and many cybercrimes are recorded as traditional crimes. An alternative is to keep traditional definitions of crime and quantify the amount of associated information and communication technologies (ICT) that each contains. This research established how much ICT was used a) in the three phases of the 'crime script' (i.e. 'before', 'during' and 'after'), b) during the criminal investigation and c) in the apprehension of the suspect(s) and d) whether digital crimes differ from traditional crimes in terms of the relationships between the victim and the offender or in terms of the physical distance between them. Residential and commercial burglary, threats and fraud were investigated and 809 incidents from the Police Department of East Netherlands were studied. It was found that ICT does not affect all types of crime equally: 16% of the threats and 41% of all frauds have partial digital modus operandi (MO). To commit burglaries, however, offenders hardly ever use ICT. In 2.9% of the residential burglaries, however, bank cards were stolen and later used to steal money from a bank account. For commercial burglary there was no associated ICT. Digital crimes differ from traditional crimes in a number of ways: the geographical distance between the victim and the offender is larger; digital threats occur relatively more often between ex-partners and digital frauds occur more often between business partners compared to traditional fraud. The study found that physical tools are more often linked to apprehension than digital ones. The regression models, however, showed digital and physical tools to be equally strong at predicting apprehension. The main findings show that ICT plays a greater role in traditional crime than expected on the basis of previous research.**

I. Introduction

The question of how much cybercrime exists is difficult to answer. The imprecision of victim surveys [1] and the unstandardized description of cybercrime incidents by commercial companies [2], [3] and the police might explain the lack of figures [4].

It seems plausible that cybercrime has become a relatively large part of overall crime. Internet use has grown rapidly. In the U.S.A, for example, 43.1% of inhabitants were internet users in 2000 and by 2010 the figure had reached 74.2%. Similarly, in The Netherlands the figures are 43.8% and 90.7% respectively [5]. Due to its widespread accessibility, the Internet has further facilitated offenses carried out with a computer. It is possible that criminals might have adapted to the increasing digitalization of society and that accordingly, cybercrime is on the increase.

Several authors consider that technology can have a profound impact on crime since it changes society; that the increased use of computers and the fact that internet connects (almost) everybody to (almost) everybody else in the world has made crime a lot easier [6], [7], [8], [9]. For instance, since the internet sometimes allows potential offenders to depersonalize victims, it might lead them to move more quickly towards actual criminal behavior [10]. An offender does not have to come face-to-face with a potential target, therefore making it easier for the offender to complete the victimization of the target [11]. In addition, all the available information present on the internet can be used for good or for evil. These developments explain the increasing interest in collecting more information on the prevalence and the characteristics of cybercrime.

There are two global approaches for the measurement of cybercrime. The first approach consists of developing a definition of cybercrime and then measuring how much crime meets this definition. This approach implies that there is 'traditional' crime on the one hand and 'cybercrime' on the other hand, meaning that cybercrime can be measured as a separate category of crime. This approach was followed by [12]. They defined cybercrime as 'the use of IT for committing criminal activities against persons, property, organizations or electronic communication networks and information systems'. [12] examined a representative sample of 13,037 crimes, as registered in the police records (10.4% of the total number of registered crimes) in the police region Zuid-Holland Zuid in 2007, and of 22,771 crimes (10.7% of the total number of cases) in the police region of Hollands Midden in 2007. In order to measure the amount of cybercrime, they used a search protocol for keywords that can be associated with cybercrime, such as 'computer', 'cyber' or 'digital'. For Hollands Midden they found 72 cases of cybercrime, which constitutes 0.32% of all registered crime; taking into account the margin of error, the amount of cybercrime was estimated to be in the range of 0.25% and 0.39%. In Zuid-Holland Zuid there were 70 cases of cybercrime, which represented 0.54% of all crime. Taking into account the margin of error, the amount of cybercrime was estimated to be in the range of 0.42% and 0.66%. The implication of this study was that the amount of cybercrime is less than 1% of the total number of crimes registered by the police.

A second approach follows a different line of reasoning. This approach focusses on the digital modus operandi (MO) of traditional crime. Most forms of cybercrime are not unique to the online world since they have long-established terrestrial counterparts [13], [14], [15] such as fraud, threats, sale of banned material and intellectual property offences. These types of offences pre-date the Internet but have found new forms of life online. Hacking activities could be seen as computer-aided versions of vandalism or trespassing. When a hacker

enters a restricted computer system, he/she is entering another person's property without authorization, which fits the definition of trespassing. Similarly, when a hacker purposely changes a website or destroys data, the action is analogous to vandalism. Several phishing schemes are basically theft. In this approach, cybercrime is essentially conventional criminal behavior that makes use of computers [16], [11]. According to this line of reasoning one might hypothesize that criminals will increasingly use ICT to commit crimes, as digitalization pervades society. The aim of the present study is to investigate how much cybercrime exists based on this second approach. The results will also elucidate whether this dichotomy of cybercrime versus traditional crime is a good reflection of reality.

Some argue that splitting crime into traditional and cybercrime has drawbacks. First, some definitions of cybercrime are narrow in focus whilst others are broad [17], [11], which hampers the comparison across countries and regions. Second, computer-related offenses are often (incorrectly) recorded as traditional crime and thus mask the extent of cybercrime. This is problematic since baseline statistics that monitor the degree to which information and communication technologies (ICT) play a role in crime are key for crime prevention. It could be therefore difficult to identify where the line that divides cyber from traditional crime lies. In addition, maybe traditional physical crime (i.e. traditional non-digital crime) itself is changing and becomes increasingly 'digital'.

There are also reasons to believe that the police systems themselves contribute to the lack of clarity between what is cyber crime and what is traditional crime. Previous research has shown that during the recording of a crime, the police sometimes ignores those ICT aspects that are less well understood. Thus fraud committed using an Internet auction such as eBay is often classified as ordinary fraud, without detailing the role ICT has played [18], [19]. Consequently, many ICT aspects of crime lie hidden in police files and that only through a detailed reading can this be elucidated. The present study was designed to examine this proposition.

There are many reasons for wanting to quantify cybercrime and its characteristics. For example, basic figures on the state of affairs are essential for policy makers. First, to guide preventive efforts, policy makers need to know how important a problem is and where it is most prominent. Similarly, to evaluate new policies or interventions, basic figures are necessary. Second, policy makers need to know how much they need to invest in extra cyber-officers and in the further training of traditional police officers. If cybercrime is low, budgets can remain low; however, if it is large and increasing, policy makers need to take action. Third, a good understanding of the modus operandi (MO) of crimes is important for the development of prevention measures. The Rational Choice Theory [20] aids situational crime prevention through its formal elaboration of the stages of the crime event (i.e. crime scripts). By setting out all the stages of a crime, it becomes easier for preventers to see possible intervention points for situational measures [21]. A script describes the MO at each step of a specific offense. In the study three stages in the execution of an offense were analyzed: the preparation of the offense (i.e. 'before'), the event itself (i.e. 'during') and after the event has taken place (i.e. 'after'). The present study describes the digital MO during these three stages of the crime.

In order to draw valid conclusions about the extent of ICT penetration into traditional crime, it is necessary to examine a representative sample of traditional offenses. In the selection of the offenses, the following considerations played a role. First, it was considered important to analyze both property as well as personal offenses. Second, it appeared relevant to analyze both an offense with a small ICT risk but also one with a large one. Accordingly, the selected offenses were: residential and commercial burglary, threats and fraud. Burglary is an 'old-fashioned' offense with unknown links to ICT. Fraud is a crime with well-known links to ICT. Threat is a personal offense which we suspect is linked to ICT.

In summary, the present study aimed to examine the extent to which ICT penetrates into 'traditional' crime in general and for the three stages of the crime script (i.e. 'before', 'during' and 'after' the event).

The contribution of this paper is to answer the following questions:

1) How much ICT has penetrated traditional crime? More specifically, how much ICT is associated with the MO 'before', 'during' and 'after' the crime?
2) Do digital crimes differ from traditional crimes in terms of the relationships between the victim and the offender or in terms of the physical distance between them?
3) How much ICT is used during the criminal investigation?
4) How much ICT led to the apprehension of suspects?
5) Which tools used in the criminal investigation are significant predictors of apprehension? Is a model based on physical tools better at predicting apprehension than one based on digital tools?

II. Method

A. The Sample

The crimes investigated are a random selection of 150 residential burglaries, 150 commercial burglaries, 300 threats and 300 fraud cases that took place in 2011 in five police forces that as of 2013 will together comprise the new regional 'Oost Nederland' (i.e. East Netherlands) police force. This region comprises 19% of the Dutch population [22]. The data was extracted from the police files between March and June 2012.

B. Procedure

Seven persons encoded information from police records using a coding list. Most cases were coded in less than 15 minutes and the maximum time required was 90 minutes. A copy of the checklist can be obtained from the second author.

Concepts:

1) Crime. Four types of crime were investigated and are hereby defined based on police definitions.
    a) Residential burglary consists of theft inside or outside the house and does not involve violence.

b) Commercial burglary consists of theft inside or outside a company or office and does not involve violence.
c) Threats consist of various sorts of intimidation actions, including stalking.
d) Fraud includes all forms of deceptive activities such as scams, counterfeiting of money or documents such as passports, identity cards, bank cards, ATM cards, checks, licenses, possession of false documents, benefit fraud, insurance fraud, false declarations and bank fraud.

2) Digital MO. The distinction between digital and traditional crime was made by identifying whether the crime was performed on the internet, whether offenders threatened to disclose digital information, whether email was sent or whether other means of digital communication were used, such as text messages. Coders had to carefully read the entire police file as this is not something that is registered in a standardized way by the Dutch police. If at least one digital MO was used, the crime was considered to be 'digital'; other crimes were therefore coded as 'traditional'.
3) Timing. To establish whether a particular act was performed 'before', 'during' or 'after' the execution of the offense, a rule was applied which took into account whether in principle, a time interval between these acts was possible. For instance, in the case of burglary, collecting information on the internet about houses that may be burgled can be done a long time in advance, therefore it is deemed to be 'before' the commission of the burglary.
4) The relationship between offender and victim consisted of different categories: a professional relationship, family, acquaintances, neighbors, ex-partners, partners, criminal contacts, on-line social network, fellow gamers, chat friends or other relationship.
5) Location was coded based on whether at the moment of the execution of the crime, the victim and the offender were: 1) both in East Netherlands, 2) either of them was in East Netherlands whilst the other elsewhere in the Netherlands, 3) both of them were outside East Netherlands, and 4) either of them was abroad.
6) Arrests. The coding consisted of whether an arrest was made and the number of persons arrested.
7) Factors that led to the arrest. It was noted whether the case was forwarded to the Public Prosecutor.
8) Tools used in the criminal investigation. The methods of detection used were noted, as well as the specific methods that led to the apprehension of the offender. A distinction was made between digital and non-digital aspects (i.e. physical).

Data reliability. Seventy cases were double coded to perform an inter-rater reliability (i.e. kappa) analysis. 24% of the variables had 'almost perfect agreement', 30% had 'excellent agreement', 22% had 'sufficient to good agreement', 4% had 'moderate' agreement whilst 20% had 'poor' agreement' (refer to [23] for inter-reliability analysis interpretation). In general the agreement for three-quarters of the variables was good to excellent which means that the results are sufficiently reliable.

C. Analyses

The data was first analyzed using cross tabulations. To investigate differences between digital and traditional crimes, a selection was made of threat and fraud cases, since only for these cases there were sufficient numbers of digital crimes available. A logistic regression was used to model apprehension on the basis of the type of tools used in the criminal investigation. Three models were generated: a digital tools, a physical tools and a combined one. The models allow to identify which individual tools are significant predictors of apprehension. It also establishes how much of the phenomenon (i.e. apprehension) can be attributed to digital or to physical tools. Furthermore, a likelihood-ratio test was used to assess whether there were any significant differences between the digital and the physical models and between the individual models and the combined or 'full' model.

III. Results

In total, 136 residential burglaries, 140 commercial burglaries, 259 threats and 274 fraud cases were coded. A number of selected cases could not be coded for various reasons. For instance, some cases were handed over to other police forces, and sometimes the cases involved a type of crime not under investigation in this study. It was possible to code information on 920 suspects and 772 victims.

Regarding the MO, a total of 16% of the threats and 41% of the frauds had a digital component (see Table I). 5.1% of the frauds involved digital burglary (i.e. hacking of systems). 2.9% of the residential burglaries involved a digital forgery. This relates to cases in which the suspect stole bank cards and withdrew money from the bank account of the victim using an ATM machine. In these cases the digital crime occurred after the first crime (i.e. third phase of the crime script). None of the cases of commercial burglary was associated to a digital MO. Threats to digitally disclose personal data occurred in only 1.9% of the cases and were always linked to the threat offense. Unsolicited emails were received in connection with threats and fraud; it occurred in 4.2% of the threat cases and in 3.6% of the fraud ones. Regarding the crime scripts in general, the highest percentage of digital MO is found in the second phase (i.e. 'during'), whilst the third phase (i.e. 'after') has the lowest percentage.

Another question is whether digital crimes differ from traditional crimes in terms of the relationships between the victim and the offender or in terms of the physical distance between them. As mentioned before, a selection was made of threats and cases of fraud. Digital offenders and traditional offenders differ with respect to the relationship with their victims. Digital threat offenders threaten their ex-partner more often (28.9%) than in the case of traditional threats (15.5%). Digital fraud occurs more often between business partners (47.3% vs. 24% for digital and traditional fraud, respectively) and occurs less often among acquaintances (1.8% vs. 7% for digital and traditional fraud, respectively).

Most threats involve persons that are both in East Netherlands at the moment of the crime. There is a trend towards

TABLE I: DIGITAL MODUS OPERANDI (MO) BY CRIME SCRIPT (N=809; in percentage)

	Residential burglary	Commercial burglary	Threats	Fraud
Digital threat				
Before ***	0	0	3.5	0
During ***	0	0	12.7	1.1
After	0	0	0.4	0.7
Total ***	0	0	14.7	1.5
Digital forgery				
Before ***	0.7	0	0.4	9.5
During ***	0.7	0	0	38.7
After *	1.5	0	0	2.9
Total ***	2.9	0	0.4	40.1
Digital burglary (i.e. hacking)				
Before n/a	0	0	0	0
During ***	0	0	0	5.1
After n/a	0	0	0	0
Total ***	0	0	0	5.1
Threat of disclosing information				
Before	0	0	0.8	0
During *	0	0	1.5	0
After n/a	0	0	0	0
Total *	0	0	1.9	0
Unwanted emails sent				
Before	0	0	0.8	1.1
During *	0	0	3.9	2.6
After [a]	0	0	1.2	0
Total *	0	0	4.2	3.6
Total ***	2.9	0	16.2	40.5
N	136.0	140.0	259.0	274.0

* Significant: $p < .05$; ** Significant: $p < .01$; *** Significant: $p < .001$
n/a: non-applicable
[a] p=0.094

an increasing geographical distance between victims and offenders when one of them was not in East Netherlands but somewhere else in the country; 19.4% for digital threats in comparison with 7.9% for traditional threats. This difference, however, is not statistically significant. 63.9% of the digital cases of fraud, but only 27.4% of traditional frauds, were committed when one of them was not in East Netherlands but somewhere else in the country. For both types of fraud, the number of international cases is low; 13.9% of the digital cases of fraud and 12.3% of the traditional cases of fraud have an international character.

In relation to the tools used in the criminal investigation, the results show that in general, physical tools are used more often than digital ones (see Table II). Physical tools are used more often for investigating burglaries than for threats and fraud. Digital tools, on the other hand, are used more often for investigating commercial burglary and fraud compared to residential burglary and threats. In the case of physical tools, the levels are similar in the case of residential and commercial burglaries (48% and 49% respectively). This is not the case, however, for digital tools since more than twice the amount of commercial burglaries (29%) used them in comparison to residential burglary (13%). Most of this difference is attributed to camera surveillance (this includes also older analog camera systems).

Regarding those factors that led to the apprehension, the results show that in general, physical factors are more often linked to apprehension than digital ones (see Table III). In the case of physical factors, it shows overall similar levels across the crime types studied. This is in contrast to the digital aspects where sharp differences are evident. For example, digital aspects led to apprehension in 3.4% of the threat cases whilst the figure is 4 times higher (14.5%) in the case of commercial burglary. This difference is considered to be exclusively due to camera surveillance and it is notable that this is the only digital aspect that is statistically significant.

This research also aimed to identify whether physical tools are better at predicting apprehension than digital ones. The regression models show that digital and physical tools explain a very similar amount of variance (21% and 22% respectively, whilst controlling for the effects of the 4 types of crimes and of witness statements). The comparison between digital and physical tools is relevant in relation to those of the descriptive statistics presented in Table II. The latter findings show that approximately twice as often are physical factors linked to apprehension than digital ones. However, as seen before, their predictive strength is very similar since there is only a 1% difference. The combined regression model shows that the digital and the physical tools used in the criminal investigation explain 23% of the variance in apprehension (see Table IV).

In relation to the tools used in the criminal investigation which significantly predict apprehension, the model (i.e. Model 1: combined) shows that physical traces of suspects predict apprehension (OR=2.10). This implies that cases that have physical traces of suspects are 2.10 times more likely to have an apprehension than those cases without physical traces. In contrast to physical tools, there are no significant digital predictors, although there is one marginally significant one (i.e. digital traces of the suspect, OR=0.58). Finally, the likelihood-ratio tests show that the addition of digital variables makes a significant contribution to an apprehension model since it tests the assumption that Model 3 (i.e. physical tools) is nested (i.e. equal to) in Model 1 (i.e. 'full' or combined model).

IV. Conclusion

This study aimed to measure the degree of ICT in traditional crimes, namely residential burglary, commercial burglary, threats, and fraud. It was found that ICT does not affect all types of crime equally: 16% of the threats and 41% of all frauds have a partial digital MO, meaning that the offenders made use of ICT in the execution of the crime. To commit burglaries, however, offenders hardly ever use ICT. It was found that 2.9% of the residential burglaries involved the theft of bank cards later used for stealing money. For commercial burglary there was no associated ICT. This overall result is more than previous research established since [12] reported that cybercrime was in the range of 0.25% and 0.66%.

Digital crimes differ from traditional crimes in terms of the relationship between the victim and the offender and in terms of the geographical distance between them. Digital threats occurred relatively often between ex-partners in comparison with traditional threats, and digital frauds occurred more often between business partners in comparison with traditional fraud. No previous studies were found that investigated this issue, therefore no comparison with the present findings was possible.

The results also show a clear geographical trend: the distance between offenders and victims increases for digital crimes as compared to traditional crimes. The fact that ICT allows a greater distance between the offender and the victim is apparent. Despite this increasing distance, international crimes

TABLE II: DIGITAL AND PHYSICAL TOOLS USED IN THE CRIMINAL INVESTIGATION (N = 809; in percentage)

	Residential burglary	**Commercial burglary**	**Threats**	**Fraud**
Physical				
Forensic investigation took place on the crime scene ***	35.3	31.4	1.2	0.4
Physical traces of the suspect found ***	39.7	43.6	14.3	7.7
Total physical***	47.8	48.6	14.3	7.7
Digital				
Digital data (e.g. Youtube-videos, chat talks, forum messages) confiscated [a]	2.2	0.7	5.0	5.1
Camera imagery confiscated ***	4.4	23.6	2.7	1.8
Phone data (e.g. locations, numbers) confiscated	5.1	7.1	5.4	2.6
Other digital traces of suspect found ***	3.7	2.1	12.0	24.8
Digital traces:, bank statement traces	0.7	0	0	1.8
Total digital***	12.5	28.6	18.1	29.4
N	136.0	140.0	259.0	274.0

* Significant: p $<$ .05; ** Significant: p $<$ .01; *** Significant: p $<$ .001
[a] p=0.076

TABLE III: SOURCE OF THE APPREHENSION (incidents with min. one apprehension; N=402; in percentage)

	Residential burglary	**Commercial burglary**	**Threats**	**Fraud**
Physical				
Statements of the suspect(s) ***	1.0	5.8	3.4	18.6
Statement of other suspect(s)*	7.1	7.6	0	2.3
Witness statements**	15.2	34.9	30.7	18.6
Statements of the victim(s) ***	17.2	11.6	51.1	7.0
DNA traces	6.1	5.2	0	7.0
Found loot **	12.1	5.8	0	0
Suspect caught in the act	36.4	37.8	35.2	39.5
Criminal Intelligence Unit information (CIE)*	0	0	0	2.3
Other **	16.2	12.8	4.5	25.6
Total physical***	78.8	83.1	85.2	88.4
Digital				
Telephone taps	1.0	0	0	0
Camera footage/imagery ***	3.0	14.5	2.3	4.7
Internet taps	0	0	1.1	0
Telephone information	2.0	0	0	0
Total digital***	6.1	14.5	3.4	4.7
N	99.0	172.0	88.0	43.0

* Significant: p $<$ .05; ** Significant: p $<$ .01; *** Significant: p $<$ .001

TABLE IV: LOGISTIC REGRESSION MODEL OF APPREHENSION IN RELATION TO THE TOOLS USED IN THE CRIMINAL INVESTIGATION (N=809). The table contains three models: individual models to predict apprehension on the basis of physical and of digital tools and a model combining both. The columns depict for each variable: the odds ratio (OR), its lower and upper 95% confidence intervals (in brackets) and its significance level.

	Model 1: combined	**Model 2: digital tools**	**Model 3: physical tools**
Forensic analysis at the scene	1.27 (0.66, 2.44)		1.24 (0.65, 2.36)
Physical traces of suspect	2.10 (1.34, 3.31)**		2.15 (1.37, 3.38)**
Digital data confiscated	0.66 (0.22, 2.00)	0.68 (0.23, 2.01)	
Camera surveillance	0.99 (0.47, 2.09)	1.02 (0.49, 2.14)	
Telecom data confiscated	1.84 (0.77, 4.38)	2.03 (0.86, 4.78)	
Digital traces of suspect	0.58 (0.30, 1.09)[a]	0.58 (0.31, 1.10)[b]	
Witness statements	1.30 (1.12, 1.53)**	1.34 (1.14, 1.56)***	1.31 (1.12, 1.53)**
Residential burglary (ref.)			
Commercial burglary	2.87 (1.62, 5.10)***	2.89 (1.65, 5.07)***	2.93 (1.68, 5.10)***
Threats	0.43 (0.26, 0.69)**	0.34 (0.22, 0.53)***	0.41 (0.25, 0.67)**
Fraud	0.23 (0.13, 0.39)***	0.18 (0.11, 0.30)***	0.20 (0.12, 0.34)***
Constant	0.61 (0.38, 0.98)*	0.82 (0.53, 1.26)	0.60 (0.38, 0.96)*

* Significant: p $<$ .05; ** Significant: p $<$ .01; *** Significant: p $<$ .001
[a] 0.092
[b] 0.092
Model 1 (p $<$.001), N=809, pseudo r2= 0.23; Model 2 (p $<$.001), N=809, pseudo r2= 0.21; Model 3 (p $<$.001), N=809, pseudo r2= 0.22
Model 1=2 (p $<$.001); Model 2=3 (p=1.000); Model 1=3 (p=0.196)

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 to a local criminal justice authority [24]. The present findings do not confirm this. A possible explanation is that it remains difficult for offenders, due to cultural and language differences, to commit international crimes.

The study found that physical tools are more often linked to apprehension than digital ones. However, the regression models show digital and physical tools to be equally strong

at predicting apprehension. In other words, physical tools are widely used. Digital ones, on the other hand, are used less often but have as strong an effect on apprehension. Camera surveillance is by far the most important digital tool that contributes to apprehension. This finding is relevant in light of the contradicting views regarding the effects of CCTV [25], [26], [27]. Physical and digital tools together explain approximately a quarter of the variance in apprehension.

Several limitations of this study should be mentioned. The sample consists of cases reported to the police in East Netherlands. The results might not be extrapolated to the country as a whole. Regional disparities exist and thus the extent to which these numbers are representative of the country as a whole must be determined. Residents of large cities are often victims of crime twice as often compared to those living in the countryside [28]. Internet use also differs by region. Residents of large cities are online more hours than those of rural areas [29], [30]. Since most large cities and urbanization in general are features of the west of the country, it seems plausible that the ICT component in the entire country would be somewhat larger than found in the present study. The present study should be extended over a larger geographic area to investigate if the differences that were found between digital and traditional offenders are confirmed.

Only four types of crime were investigated, namely residential and commercial burglary, fraud and threats. Future research should investigate other types of crime.

The information is based on victim reports as registered by the police and doubt exists as to how accurate these are particularly in relation to the digital nature of crimes. However, based on our reading of the files [31], it appears likely that the police do not accurately register digital MO. This could imply that the figures of digital crime might actually be higher. Another limitation is that, for some crimes, the MO is unknown. For instance, sometimes police officers found that burglars used Google Maps and information from websites to identify and burgle wealthy houses. The present study did not find evidence of this type of digital preparation. However, even if offenders used these digital MO's, it is unlikely that the victims were aware of it, which means that it went unnoticed unless an apprehension occured.

A further limitation is that the findings are partly analysed 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 crimes that are representative of the population from which they were chosen, namely burglaries, threats and fraud cases in East Netherlands. It should be noted that burglaries, threats and fraud cases have a high incidence. In 2010, out of the total number of recorded crimes, 10% were residential burglaries whilst 19% were commercial and other forms of burglary [28], 4% were threats and finally 3% were fraud. The types of crimes investigated therefore constitute 36% of the recorded criminal activity of The Netherlands.

An interesting issue that this research did not set itself to answer but that is a relevant follow-up study is how the relationship between ICT and traditional crime evolves in time and how it compares to that of cybercrime. In addition, it would be important to identify whether any changes found would be attributable to offender and victim behavior or to police recording and investigation practices.

ACKNOWLEDGMENT

This research was funded by the Cybercrime program (Programma Aanpak Cybercrime (PAC)) of the Dutch police.

REFERENCES

[1] R. Anderson, C. Barton, R. Bohme, R. Clayton, M. vanEeten, M. Levi, T. Moore, and S. Savage, "11th annual workshop on the economics of information security,," in *WEIS 2012*.

[2] Verizon-Risk-Team, "2013 the 2013 data breach investigations report," Verizon, Tech. Rep., 2012.

[3] Tech. Rep.

[4] B. of Justice-Statistics, "Ic3 2011 internet crime report," Tech. Rep., 2011.

[5] The-World-Bank, "Internet users (per 100 people)," 25 March 2013 2013.

[6] J. S. Albanese, "The causes oforganized crime. do criminals organize around opportunities for crime or do criminal opportunities create new offenders?" *Journal of Contemporary Criminal Justice*, vol. 16, no. 4, pp. 409–423, 2000.

[7] R. V. Clarke, "Technology, criminology and crime science," *European Journal on Criminal Policy and Research*, vol. 10, no. 1, pp. 55–63, 2004.

[8] M. Felson, *Crime and Nature*. Thousands Oaks, CA: Pine Forge Press, 2006.

[9] M. Felson and R. V. Clarke, "Opportunity makes the thief practical theory for crime prevention," Home Office, Tech. Rep. 98, 1998.

[10] N. Selwyn, "A safe haven for misbehaving?: An investigation of online misbehavior among university students," *Social Science Computer Review*, vol. 26, no. 4, pp. 446–465, 2008.

[11] T. A. Petee, J. Corzine, L. Huff-Corzine, J. Clifford, and G. Weaver, "Defining "cyber-crime": Issues in determining the nature and scope of computer-related offenses," in *Futures Working Group*, T. Finnie, T. Petee, and J. Jarvis, Eds., vol. 5, 2010, pp. 6–11.

[12] M. Domenie, E. Leukfeldt, M. Toutenhoofd-Visser, and W. P. Stol, "Werkaanbod cybercrime bij de politie: een verkennend onderzoek naar de omvang van het geregistreerde werkaanbod cybercrime," Lectoraat Cybersafety, Noordelijke Hogeschool Leeuwarden, Tech. Rep., 23 March 2009 2009.

[13] P. N. Grabosky, "Virtual criminality: Old wine in new bottles?" *Social and Legal Studies*, vol. 10, no. 2, pp. 243–249, 2001.

[14] R. McCusker, "Transnational organised cyber crime: Distinguishing threat from reality," *Crime, Law and Social Change*, vol. 46, no. 4-5, pp. 257–273, 2006.

[15] R. Neve and R. van der Hulst, "High-tech crime: Inventarisatie van literatuur over soorten criminaliteit en hun daders," WODC, Tech. Rep. 978-90-5454-998-7, 2008.

[16] Q. Li, "New bottle but old wine: A research of cyberbullying in schools," *Computers in Human Behavior*, vol. 23, no. 4, pp. 1777–1791, 2007.

[17] S. Gordon and R. Ford, "On the definition and classification of cybercrime," *Journal in Computer Virology*, vol. 2, no. 1, pp. 13–20, 2006.

[18] P. H. Hartel, M. Junger, and R. J. Wieringa, "Cyber-crime science = crime science + information security," CTIT, University of Twente, Technical Report TR-CTIT-10-34, Oct 2010. [Online]. Available: http://eprints.eemcs.utwente.nl/18500/

[19] D. S. Wall, *Cybercrime: The Transformation of Crime in the Information Age*. Cambridge, United Kingdom: Polity, 2007.

[20] D. B. Cornish and R. V. Clarke, *The Rational Choice Perspective*. Cullompton UK: WillanPublishing, 2008.

[21] M. J. Smith and R. V. Clarke, *Situational Crime Prevention: Classifying Techniques Using 'Good Enough' Theory*, 2012.

[22] CBS, "Bevolking; geslacht, leeftijd, burgerlijke staat en regio, 1 januari (population, gender, age, marital status and region, 1 january)," March 4, 2013.

[23] J. R. Landis and G. G. Koch, "The measurement of observer agreement for categorical data," *Biometrics*, vol. 33, no. 1, pp. 159–174, 1977.

[24] J. Barham, "International cybercrime. russia's cybercrime haven," 2013.

[25] M. Gill, A. Spriggs, J. Allen, J. Argomaniz, J. Bryan, P. Jessiman, D. Kara, J. Kilworth, R. Little, D. Swain, and S. Waples, "The impact of cctv: Fourteen case studies," Research Development and Statistics Directorate, UK Home Office, Tech. Rep., 2005.

[26] L. Van Noije and K. Wittebrood, "Sociale veiligheid ontsleuteld: Veronderstelde en werkelijke effecten van veiligheidsbelied," Sociaal en Cutureel Planbureau, Tech. Rep., 2008.

[27] B. Welsh and D. Farrington, "Effects of closed circuit television surveillance on crime," The Campbell Collaboration, Tech. Rep., 2008.

[28] A. Eggen and R. Kessels, *Criminaliteit en Opsporing*. The Hague, The Netherlands: Boom Juridische Uitgevers, 2011.

[29] A. v. d. Broek, K. Breedveld, J. d. Haan, L. Harms, and F. Huysmans, *Tijd en Vrije Tijd*. The Hague, The Netherlands: Sociaal Cultureel Planbureau, 2006, pp. 289–316.

[30] S. Kalidien, N. d. Heer-de Lange, and M. v. Rosmalen, *Criminaliteit en Rechtshandhaving 2010: Ontwikkelingen en Samenhangen*. The Hague, The Netherlands: Boom Juridische Uitgevers, 2011.

[31] M. Junger, A. L. Montoya Morales, P. H. Hartel, and M. Karemaker, "Modus operandi onderzoek naar door informatie en communicatie technologie (ict) gefaciliteerde criminaliteit," http://eprints.eemcs.utwente.nl/23227/, Centre for Telematics and Information Technology, University of Twente, Enschede, Technical Report TR-CTIT-13-07, January 2013.