Copyright © 2013 International Journal of Cyber Criminology (IJCC) ISSN: 0974 – 2891
January – June 2013, Vol 7 (1): 1–17

High Volume Cyber Crime and the Organization of the Police: The results of two empirical studies in the Netherlands

Rutger Leukfeldt,[1] **Sander Veenstra**[2] **& Wouter Stol**[3]
NHL University of Applied Sciences, The Netherlands

Abstract

The question that is central in this paper is: to what extent is the Dutch police organization able to effectively combat high volume cyber crime? First we focus on the definition of cyber crime in the Netherlands. Next, we examine the criminalization of the two most common cyber crimes in the Netherlands: hacking and e-fraud. After that, based on police records, we analyze the nature of these crimes. Thereafter, we will look at the functioning of the Dutch police regarding cyber crime. What are the strengths and weaknesses of their handling of cyber crimes? We conclude that the Dutch police are insufficiently organized to combat cyber crime. The lack of priority and proper capacity throughout the entire police organization to fight digital crimes results in cyber cases never entering the criminal justice system or leaving the criminal justice process early.

Keywords: cyber crime, hacking, e-fraud, police, policing, organization.

Introduction

To be able to function in a good and orderly way, society needs some degree of order and continuity, and therefore safety. Safety and security has long been merely a question of protection against dangers from the physical world. Late last century, 'cyberspace' arose alongside the old world (Stol, 2008). This 'new' world is increasingly intertwined with the traditional offline world and therefore safety in cyberspace has become a prerequisite for a well-functioning society. A secure cyberspace means a cyberspace where (and from where) no crime is committed. In this, the police have a task.

Although the essence of police work has remained the same over the years - to maintain the law and provide assistance to those who need it - a changing society requires continuous change in the police organization (Van der Vijver & Terpstra, 2007). From

[1] Researcher, Cybersafety Research Group, Institute for Business and Management, NHL University of Applied Sciences, P.O. Box 1080, 8900 CB Leeuwarden, The Netherlands. Email: e.r.leukfeldt@nhl.nl

[2] Researcher, Cybersafety Research Group, Institute for Business and Management, NHL University of Applied Sciences, P.O. Box 1080, 8900 CB Leeuwarden, The Netherlands.

[3] Professor at Open University of the Netherlands and Chair holder, Cybersafety Research Group, Institute for Business and Management, NHL University of Applied Sciences, P.O. Box 1080, 8900 CB Leeuwarden, The Netherlands. Email: W.PH.Stol@ecma.nhl.nl

organizational theories, we have known for some time that there is no one best way of structuring an organization and that organizations to a significant degree are controlled by external powers (Lammers, 1983; Pfeffer & Salancik, 1978; Grusky & Miller, 1981). Therefore, organizations must adapt to their environment in order to be as effective as possible. This also applies to the police. In the past, for example, the Dutch police had to adapt her organization to the former community policing philosophy and, indeed, did so with a certain level of success (Cozijnsen, 1989). Today's local police officer not only has to know his neighborhood, but also digital playgrounds and hangouts.

The question that is central in this paper is: to what extent is the Dutch police organization able to effectively combat cyber crime? First we focus on the definition of cyber crime in the Netherlands and discussions on this subject. Next, we examine the criminalization of the two most common cyber crimes in the Netherlands: hacking and e-fraud. These are the two offenses that confront the police the most. The penalization of these offenses determines whether and how the police deal with them. After that, based on police records, we analyze the nature of hacking and e-fraud cases that the police have to deal with. We want to know more about this new workload and the specific characteristics of offences and offenders. Apart from penalization of offenses, it is also the nature of cyber crimes that determines how the police as an organization must structure itself. Does it, for instance, involve crimes with a high number of suspects who are collaborating internationally? Or do teams mainly have to deal with minor crime happening within the region? Thereafter, we will look at the functioning of the Dutch police regarding cyber crime. What are the strengths and weaknesses of their handling of cyber crimes? In the final section, we conclude that the Dutch police, except for some specialized teams, are insufficiently organized to combat cyber crime. Although most of these cyber crimes are still committed from within the country, hacking and e-fraud are internationalizing everyday police work. Furthermore, the police will have to deal with cyber crime more often and throughout their organization. However, the lack of priority and proper capacity throughout the entire police organization to fight digital crimes results in cyber cases never entering the criminal justice system or leaving the criminal justice process early.

Cyber crime: the Dutch definition

There is no consensus in the Netherlands on how cyber crime should be defined and which crimes it encompasses exactly. In their literature study, Van der Hulst and Neve (2008, p. 19) concluded that: 'A common definition and consistent conceptual framework is lacking for this field of crime. A veritable arsenal of terminology is used, sometimes in combination with the prefixes cyber, computer, e-, internet, digital or information. Terms are bandied around, applied randomly, reflect overlap in content or reflect important gaps.' In this section, we will discuss a number of definitions used in the Netherlands.

From an inventory compiled by the Cyber Crime Programme of the Dutch police force [in Dutch: *Programma Aanpak Cybercrime*], it is clear that in the Netherlands significant differences exists in the scope of the definitions used, and with this the types of crime that do, and do not, fall within its meaning. Definitions range, for instance, from: 'any kind of crime that is related to computer systems', to 'all crime carried out using a digital component' (PAC, 2008, p.1). It is clear that these definitions differ somewhat in their nature. The first definition is narrow: only crimes that are committed on computer systems, for instance, hacking and spreading viruses, are included, while crimes like fraud or stalking via internet are not. The second definition is broad: crimes whereby the perpetrator has merely used a mobile phone or a satellite navigation system to commit them are also considered to be cyber crime.

There are also several definitions that fall between these two extremes. Characteristic of these definitions is that they identify several categories (Van der Hulst & Neve, 2008; Stol et al., 2011; Leukfeldt et al., 2010, 2012, 2013; Bernaards et al., 2012; Campman, 2012; Domenie et al., 2013). The common theme here is that there is a category of offenses that focuses on Information and Telecommunication Technology (ICT) and these offenses are committed using ICT (hacking, destruction of digital information). Furthermore, there are offenses that do not focus on ICT, but in which ICT is fundamentally important to enabling the offence to be (for instance, fraud via internet or the spreading of child pornography).

Although the latter categorization is used the most to define cyber crime and to classify types of online crime, discussions are still on-going. Within the criminal justice system, there is no consensus about whether cyber crime in the broader sense of the word should be defined as cyber criminality (see also Stol et al., 2011, Campman, 2012, Bernaards et al., 2012, Leukfeldt et al., 2010, 2012, 2013, Domenie et al., 2013). The issue is whether there is evidence of a new kind of crime that demands new methods of criminal prosecution – which is not uncommon in cases of cyber crime in the narrow sense – or whether it merely involves pre-existing kinds of crime that are being committed using new means. The latter do not call for significant changes to the criminal justice system. However, the discussion about the definition to be used has not yet ended.

Therefore, in this paper ‘cyber crime’ is defined as the overarching concept for all kinds of crime whereby ICT plays a significant role in the committing of the offence. Two subcategories are distinguished here: crimes in which ICT is both the instrument and the target (cyber crime in the narrow sense), and crimes in which ICT is fundamentally important for its execution, but in which ICT is not the target (cyber crime in broader sense).

This paper uses ‘cyber crime’ as a general term for all forms of crime in which ICT plays an essential role. Many crimes fall within this definition. Leukfeldt et al. (2012) describe, for instance, the penalization of 28 crimes, ranging from hacking digital systems and installing spy ware to fraud using internet banking and cyber stalking.

Two most common cyber crimes in the Netherlands

The two crimes that are discussed in this paper are hacking and e-fraud. Dutch citizens are most likely to fall victim to these crimes. In 2011, the first victim survey on cyber crime in the Netherlands revealed that 4.3 per cent of the Dutch population aged 15 and above fell victim to hacking (Domenie et al., 2013). In addition, 3.5 per cent of the population fell victim to e-fraud. Compared to the results of the traditional Dutch victim survey in the same year (CBS, 2012), only bicycle theft occurred more frequently (4.8 per cent). Other offline crimes occur far less frequently: 1 per cent fell victim to physical abuse, 1.2 per cent to burglary and 1.5 per cent to sexual offenses.

Indeed, hacking and e-fraud are the most prevalent cyber crimes in the Netherlands. These cyber crimes have become high volume crimes. Moreover, these crimes are interesting to study because of other aspects too. Firstly, hacking can be regarded as a basic offense because it is a gateway to other types of crime (Leukfeldt et al., 2010; KLPD, 2007; Bernaards, 2012; Domenie et al., 2013). Furthermore, with the advent of the internet and the e-commerce economy, new ways of committing fraud have emerged. E-commerce is a rapidly growing sector that handles a lot of money. The easy access and global reach of the internet provides many opportunities to sell and purchase products and services. The number of Dutch people shopping online has grown to 9.5 million in 2011 (on a total population of 16.6 million). In that year, 6.7 million people *frequently* ordered goods and / or services over the Internet (CBS 2012). Websites like eBay and other auction or selling sites have created a lively trade between individuals. eBay has over 100 million active users globally and in 2012, the total worth of goods sold on eBay was $68.6 billion.[4] The economic sector has become increasingly dependent on online business traffic. Internet is now part of what is called the vital infrastructure for economic processes (Helmus et al. 2006; KLPD, 2004). Loss of trust in the e-commerce sector can have major consequences for the economy and society as a whole (Sackers & Mevis, 2000).

Hacking and e-fraud: Penalization in the Netherlands[5]

Hacking and e-fraud are the two cyber crimes to which members of the public in the Netherlands are most likely to fall victim to. Because of this, the police have to deal with these offenses most frequently. This has also been shown to be the case by previous research into the cyber crime-related workload in the Netherlands (Domenie et al. 2009). Before we discuss the nature of these two crimes, we will show how these cyber crimes are penalized in the Netherlands. After all, if the legislation in this area is inadequate or lacking altogether, then it will have no impact on how the police deal with these cyber crimes.

Hacking

From a legal point of view, hacking involves gaining access to a computerised work without permission (Article 138ab Dutch Penal Code [*Wetboek van Strafrecht* (Sr)]). This has to involve intentional and unlawful entry into a computerized work or part thereof. The perpetrator must have the intention of breaking into the system, and this entry must be unlawful. If someone gains access to the account of another without permission, this is known as hacking, even if that person guesses the password, and even if that person could have gained access anyway. Someone who accidentally ends up in another person's computer system is not punishable.

Two terms are important here: computerized work and breaking into (forced entry). According to the Dutch law, a computerized work is a system that is intended to store, process and transfer information using electronic means, for instance, a computer, a database or a server on which websites are hosted (Sect. 80e Sr). 'Forced entry' is in any event involved, according to the law, if access to the system is gained through: (a) breaching security, (b) a technical intervention, (c) using fake signals or fake keys, or (d) by adopting a false identity. The words 'in any event' indicate that the list is not definitive. By adding these words, the legislature allowed for the possibility that previously unemployed tricks would still constitute hacking (Dijkstra, 2008).

Acts of preparation for hacking may also be punishable. Selling, acquiring, spreading or in other respects making available or possessing a password, code or similar data, which will enable access to a computerized work, with the aim of hacking, intercepting or acquiring information is punishable according to Paper 139d paragraph 2(b). As a

[4] http://www.ebayinc.com/who. Last visited at January 24th 2013.

[5] Based on Leukfeldt e.a. (2012).

consequence, anyone that tricks or cheats another person into revealing their password ('acquiring', for instance, through social engineering), with the intention of hacking that person's computer, is therefore punishable. In addition to this, anyone that creates, possesses or spreads key loggers or certain other kinds of malware is also punishable (Article 139d paragraph 2 Sr).

E-fraud

Although there are many different kinds of e-fraud (online sale and auction fraud, identity theft and abuse (phishing, skimming), Nigerian scams, etc.), two sections of the Dutch Penal Code play an important role regarding all these kinds. Section 326 Sr (fraud) makes scams punishable which are aimed at gaining unlawful benefits. Among other things, Section 326 Sr covers fraud that leads to the delivery of goods, including money transfers and cash payments (notes and coins). In addition to this, the intentional use of fake or forged documents as though they were real and genuine is punishable (Section 225 paragraph 2 Sr). It is also punishable to intentionally submit or be in the possession of a fake or forged document while being aware or reasonably suspecting that this document is intended to be used as though real and genuine (Section 225 paragraph 2 Sr). On the grounds of Section 225 paragraph 1 Sr, it is punishable to forge or counterfeit ('to prepare falsely') any document that is intended to serve a proof of any fact. Forging and counterfeiting is only punishable if the perpetrator intends to use the document as 'genuine and unfalsified' themselves or have others use them as such.

The term 'document' is interpreted broadly. Computer data that are readable or can be rendered readable relatively easily, and have been recorded in a relatively fixed way (i.e. with the intention of being stored, temporarily or not) constitute a document.[6] This applies, for instance, to emails, web pages and most computer files. This does not mean that they necessarily fall under Section 225 Sr; for this the requirement is that they also have to serve as evidence ('that according to generally accepted standards usually serve as evidence of any fact').[7]

In addition, various other sections of the law may be relevant. For instance, identity abuse (intended for committing fraud) is not provided for in the Criminal Code; instead it falls under the previously mentioned Sections 326 Sr and 225 Sr. Acts intended to obtain an identity, however, can be punishable. It is possible for criminals to get their hands on identity information by breaking into computer systems. Acts like this constitute hacking (Section 138ab) and, subsequent to hacking, assuming, intercepting and taking information are also punishable (Section 138ab paragraph 2 Sr). Section 139c Sr applies to the intentional and unlawful intercepting or taking of personal data, using a technical device (for instance, spy ware or a key logger). Having another person's identity information, or fictitious identity information, is in itself not always punishable, but it is if these are obtained by unlawfully intercepting or taking information, including from a computer (Section 138ab paragraph 2 Sr, Section 139c Sr and Section 273d paragraph 1(a) Sr). It is also punishable to reveal this information to another person, and to have or to intentionally make available to another person, the object on which information is stored (Section 139e Sr).

[6] Supreme Court 15 January 1991, Dutch Law Reports 1991, 688; more generally: Parliamentary Papers II 2002/03, 29 025, no. 3, p. 3.

[7] Supreme Court 30 September 1980, Dutch Law Reports 1981, 70; Supreme Court 20 April 2004, 681.

Methodology

E-fraud and hacking occur relatively frequently, and given that they are offenses punishable by law, investigating them is a matter for the police. In next sections of this paper we describe the extent to which the police are capable of effectively tackling these cyber crimes. However, before we describe these findings, we will first give an account of the methodology we used.

This paper is based on two empirical studies in the Netherlands. An explorative study into the nature of cyber crime in Dutch police files (Leukfeldt, Domenie & Stol, 2010) and a study into the functioning of the Dutch criminal justice system regarding cyber crime (Leukfeldt, Veenstra, Domenie & Stol, 2013). The study of Leukfeldt et al (2010) is an exploration in the area of cyber crime and offers insight into forms of cyber crime that are most relevant for the police. Key research questions are: (1) What is the nature of these cyber crimes? (2) What is known about the perpetrators? To answer these research questions different research methods were used. The study started with a literature review. The purpose was to create insight into the nature of the cyber crimes and their offenders and to develop an analytical framework. Through (online) libraries, books, papers and reports on the subjects were retrieved and relevant publications were studied. The second method was a file study. The framework was used to analyze police files regarding cyber crimes. We analyzed existing data in police records in cooperation with the Dutch National Police. Based on keywords, we selected files from the basic registering system (BPS)[8] of the Dutch police from the period 2002 – 2007. The advantage of using slightly older files is that the police will have had enough time to investigate the case and to put information in the files that can be used for analysis. The files that were selected in this way were read by the researchers to determine if they really involved cyber crimes. Five student assistants then analyzed these files using a standard protocol developed by the researchers.

Remarkably little social scientific research has been done into cyber crime. The exploratory research of Leukfeldt et al., (2010) was done to improve understanding of the nature of cyber crime in the Netherlands and its perpetrators. During the study, it appeared that cyber crime cases often lack information, especially on techniques used, like social engineering, phishing and key loggers. Toutenhoofd et al., (2009) conclude in their study that police personnel responsible for the registration of crime often lack knowledge about cyber crime. A limitation of this study, therefore, is that it is based on police files, which means that valuable information is sometimes missing. We want to emphasize that the analysis was done over files from Dutch police regions. Files from the specialized national Team High Tech Crime (THTC) were not included. We did this for two reasons: Firstly, during the file study, the THTC had just been set up. The team had not handled many cases yet. Secondly, we wanted to examine cyber crimes regular police teams have to deal with. The analysis of files of specialized teams would not help to obtain a clear image of the workload of these police teams.

The main goal of the second study (Leukfeldt et al 2013) was to, both quantitatively as well as qualitatively, describe (points for improvement in) the way the Dutch criminal justice system handles crime in the digital era. Therefore, the cyber crime cases which were studied to reveal the nature of cyber crime in Dutch police reports (Leukfeldt et al

[8] The BPS system includes a register of all the actions of police officers (for example taking victims' statements or hearing suspects). It includes persons who are only a suspect and who have not yet been convicted.

2010) were followed throughout the criminal justice process and 30 interviews with key figures within the criminal justice process were held. The quantitative research revealed that following cases within the Dutch criminal justice system is problematic. The administrations of the police, the prosecution service and the judiciary are incomplete and do not match adequately. In previous research a similar conclusion was drawn with regard to other forms of crime (Algemene Rekenkamer, 2012; Leertouwer & Kalidien, 2011). As a result, it has only been possible to quantitatively reveal how the police handle cyber crime. Nevertheless, the interviews have given insight into (points for improvement in) the functioning of the Dutch criminal justice system in the digital era.

Ethical issues

Both studies were conducted under the research ethics code of the Cyber Safety group of the NHL University of Applied Sciences and the Dutch Police Academy. The code is based on the ethics code according to which scientific research has to be conducted in The Netherlands (KNAW, 2003). Therefore, the research was executed in accordance with scientific rules of accountability, diligence, impartiality, integrity and confidentiality.

Furthermore, the study of Leukfeldt et al (2010) deals with some specific ethical issues. During the file study, the researchers and student assistants had access to personal data of offenders and victims who were registered in the basic registering system (BPS) and the criminal convictions database (HKS). Articles 4.1 – 4.5 of the above mentioned research ethics code apply here. In order to analyze police files, the researchers and student assistants first had to get permission from the Dutch Justice department. This department reviewed the research proposal and checked its scientific relevance. Furthermore, the researchers were screened by the Dutch police: a check was carried out to see if they had criminal records and researchers and student assistants were assessed to see whether they were vulnerable to extortion or bribery. Information about the first and last name of the offenders was not extracted from the police files. Only anonymous information was used in the final report. Therefore, it was not possible to track down persons based on the data in the report. Furthermore the researchers did not contact persons mentioned in police records.

Hacking and e-fraud in the Netherlands

In this part of the paper, the results of the empirical study into cyber crime (Leukfeldt et al., 2010) are presented. The modus operandi and the characteristics of suspects of hacking and e-fraud cases in the Netherlands will be described. The nature of the cyber crime is, after all, a determining factor for how the police organization should be structured. Does it, for instance, involve crimes with a high number of suspects who are collaborating internationally? Or do teams mainly have to deal with minor crime happening within the region?

The nature of cyber crimes

Modus operandi

In order to determine the modus operandi of cyber crimes offenders, we analyzed the (1) preparations undertaken (2) criminal methods, (3) number of (cooperating) suspects and (4) the country from where the suspects operated.

(1) Preparations undertaken

Cyber criminals undertake various preparations prior to committing their crimes. In 28 hacking cases (20.1%) suspects made preparations. Examples are writing or downloading a program that takes advantage of weaknesses in a computer system, or collecting information about a victim to be able to retrieve their password. Many of the hacking cases appeared to lie within the social sphere. The goal of the hacking was often just to antagonize someone (see for example Case 1). Hacking in most cases is not so much the goal, but is itself a preparatory act for some other form of crime.

Case 1: Hacking in the relational sphere

> I was married to [suspect]. On [date] I officially divorced [suspect]. After the official divorce comes the process of determining the alimony. From [date] I noticed that my personal and private data was known to [suspect]. I received a letter from my neighbor with an incriminating statement that I wanted to use in court. This (paper) letter I personally received at another location because I did not want to arouse suspicion. On [date] I digitized the letter and stored it on my laptop. After that, I sent it over a wireless network to my lawyer. On [date] my neighbors called me and told me that my ex, [suspect], stood at their doorstep and wanted to know about their incriminating statement. [Suspect] had information from the letter I had sent to my lawyer. There were also some e-mails deleted from my e-mail account and [suspect] knew about other confidential information about me and correspondence with my lawyer. I suspect that my ex-partner may have had access to my laptop, possibly by hiring a hacker. The reason that my ex-partner would do this is because she wants to manipulate the judicial process by passing on my incriminating statements to her lawyer.

In 71 of the e-fraud cases (22.6%) suspects made preparations: 39 incidents (54.9%) of placing advertisements on a sales site, possibly in conjunction with creating a false identity and an account into which the money could be paid (Case 2). In 13 cases (18.3%) the suspects created a website and an e-mail address to scam people. The website was designed to look like a legitimate business. In two other cases the suspect sent genuine looking e-mails (e.g. advertising or promotions). In one case the suspect sent e-mails to gain personal information (including username and password of a PayPal account). In four cases, a false identity was created. In two cases, the suspects had stolen credit card information in order to make purchases over the Internet. In the remaining 10 cases it was unknown which preparatory acts the suspects made.

Case 2: E-fraud

> I want to report a scam. On the Internet, on the selling site 'marksplaats.nl', from [date] a telephone was offered. The asking price was 120 euro. I was interested in the product. I sent an e-mail saying that I agreed to the asking price. I then transferred money to [suspect]. The suspect told me that I would receive a track and trace code. I've never been given the code. Subsequent correspondence was only to apologize. The advertiser pretended to live in Belgium, but I don't think this is true. The telephone I ordered and paid for were never delivered. I think I was scammed, especially since the telephone was offered again on the Internet.

(2) Criminal methods

In 86 hacking cases (61.9%), suspects made use of various criminal techniques. In 60 of the 86 cases (69.8%) in which information about the use of criminal techniques existed, it was clear that a criminal technique was used, but we could not find information on what it was exactly. An example: the username and password of a victim were used to break into a computer, but it is not known how these credentials were obtained. We know which techniques were used in 26 of the cases. The most common technique is defacing websites (61.5%) (see Case 3). Most defacing cases involved the unauthorized modification of personal pages on social networking sites (such as inserting defamatory pictures or texts onto someone's account). Other techniques that we found in the files were key loggers (23.1%) and phishing sites (19.2%). The police files that we studied did not contain other techniques.

Case 3: Defacing website

I want to declare the intentional and unlawful disposal and modification of data. I am a professional consultant and I have my own website. On [date], an unknown person hacked my site and changed and deleted data. This lasted two days. Subsequently, the suspect deleted all my data. All of this has led to reputation damage and financial loss. First of all because my website had to be repaired. Second, because customers could read on my site that I was hacked.

In 43 e-fraud cases (13.7%), we found that one or more criminal techniques were used. In nine of these cases it was not clear precisely which technique was used. In 32 of the 34 remaining cases (94.1%) the suspect used social engineering: persuading a user to do something he would normally not do. In two cases (5.9%) phishing was used: criminals get hold of their victims' credentials by using a fake website and then use this information to commit e-fraud. It is conceivable that cyber criminals use this technique without their victims noticing that their data has been pilfered, in which case victims cannot report anything.

(3) Suspects

For each case, we noted the number of suspects (Table 1). In most cases there was one suspect. In some cases there were two suspects; there were hardly any cases with more than two suspects.

Table 1: Number of suspects per case

	Hacking (n=54)	*E-fraud (n=217)*
Number of suspects	*%*	*%*
1	*83.1*	*81.6*
2	*13.8*	*12.0*
3	*1.5*	*4.1*
4	*0.0*	*1.4*
5	*1.5*	*0.0*
6	*0.0*	*0.5*
7	*0.0*	*0.5*
Total	*99.9*	*100.1*

The fact that more than one suspect is listed in a case does not mean that they are acquaintances of each other or that they have cooperated. Most cases do not involve organized crime or suspects who are working together[9]. Sometimes, organized groups are involved in hacking and e-fraud cases. In 4.6% of the hacking cases, suspects are part of a criminal group who know each other and work together. The case study shows that hacking is an offense that is usually committed outside organized crime groups. Furthermore, in 2.2% of e-fraud cases the offense may have been committed by an organized group. An example is a group of suspects who scammed people by using a fake company to sell and never deliver goods. There are also examples of advance fee fraud: the victims were told that they had won a luxury cruise and only had to pay a deposit. E-fraud is similar to hacking in that most offenses are not committed by organized groups.

(4) Countries of suspects operation

Although in most cases in our study, suspects were operating from the Netherlands, some criminals operated from abroad:

- 23.4% of the 60 hacking files;
- 14.5% of the 166 e-fraud cases;

Although most suspects operate from the Netherlands, almost a quarter of hacking crimes were committed from across the border. We have no figures about normal (offline) crime cases, but, as we see it, in these cases the police are unlikely to have to deal with as many suspects from abroad as they would in hacking (23.4%) and e-fraud (14.5%) cases.

Offender characteristics

Gender was known for 281 suspects (Table 2). The division between men and women in cyber crime cases differs significantly from the standard distribution of the total population ($p < 0.01$): men are overrepresented. While cyber crime suspects are generally far more likely to be male than female, the percentage of men committing e-fraud (73.4) is lower than the averaged Dutch suspect (HKS) (82.9) ($p < 0.01$). Indeed, e-fraud, usually a scam done on online marketplaces, is a crime committed by relatively more women than usual.

[9] From an international point of view, there is no consensus about the definition of organized crime. For instance, Klaus von Lampe, Professor of Organized Crime at the John Jay College of Criminal Justice, New York, gathered more than 160 international definitions (www.organized-crime.de/organizedcrimedefinitions.htm. Retrieved on 16 July 2012.) In the Netherlands there is a generally accepted definition of organized crime. The definition was developed by the Fijnaut research group that was commissioned by the Parliamentary Committee of Inquiry into Investigation Methods to study organised crime in the Netherlands. The researchers define organized crime as groups that primarily aim at illegal gain, commit offences systematically with serious consequences for society, and are capable of concealing these offenses in a reasonably effective way (PEO, Appendix VII, 1996, p. 24). In the years that followed, this definition was adopted by researchers who charted organized crime in the Netherlands empirically (Kleemans, Brienen & Van der Bunt, 2002; De Bunt & Kleemans, 2007). It was also adopted by Van der Hulst and Neve (2008) who inventorized international literature regarding organized cyber crime.

Table 2: Gender of suspects

	Hacking (n=63)	*E-fraud (n=218)*	*# HKS (n=244.000)*	*## NL (n=16mlj)*
Gender	*%*	*%*	*%*	*%*
Men	79.4	• 73.4	82.9	⋆ 49.5
Women	20.6	26.6	17.1	50.5
Total	100.0	100.0	100.0	100.0

# Source: Prins, 2008; ## Source: www.cbs.nl, reference year = 2009.
⋆ Significant difference with all the other percentages in that row;
• Significant difference with HKS (always p<0.01).

The age was known of 251 suspects. The youngest is 13 and the oldest 73 years old. Table 2 shows the distribution of age groups and includes the age distribution of the Dutch population aged 12 years and older,[10] and the age distribution of all suspects in the HKS database ('the average Dutch suspect').

To begin with, we see that the age distribution of cyber crime suspects differs significantly from the age distribution of the normal Dutch population. Almost half (45.9%) of e-fraud suspects, for example, are between 18 and 24 years old, while only 24.6% of the Dutch population of 12 years and older falls in this age category. HKS suspects in the age categories between 12 to 44 years are overrepresented. Crime is mainly committed by men who are less than 45 years of age. Overall, youngsters are overrepresented in our study.

Compared to the Dutch population, hacking suspects are more likely to be aged between 12-24 years (42.6% of hacking). For some age categories of 24 years and older, there are no significant differences in terms of age distribution compared to the normal Dutch population. The oldest one or two categories are underrepresented.

Table 3: Age distribution of suspects, compared with Dutch suspects and the Dutch population

	Hacking (n=47)	*E-fraud (n=194)*	*HKS # (n=244.000)*	*NL-12+ ## (n=14mlj)*
Age category	*%*	*%*	*%*	*%*
12-17 years	⋆ 21.3	• 5.2	14.4	X 8.6
18-24 years	⋆ 21.3	•⋆ 45.9	24.6	X 9.7
25-34 years	17.0	•⋆ 33.0	21.8	X 14.7
35-44 years	25.5	•⋆ 10.3	19.7	X 18.6
45-54 years	10.6	•⋆ 4.6	11.7	X 16.9
55-65 years	4.3	•⋆ 0.5	5.4	X 14.5
65 years and older	⋆ 0.0	⋆ 0.5	2.3	X 16.9
Total	100.0	100.0	99.9	99.9

# Source: Prins, 2008; ## Source: www.cbs.nl, reference year = 2009.
⋆ Significant difference compared to Dutch population;
• Significant difference compared to HKS;
x Significant differences between HKS and the Dutch population (always p<0.01).

[10] We compare our data with the Dutch population of 12 years and older since in The Netherlands people less than 12 years old cannot be prosecuted and, consequently, our data is limited to people aged 12 years and older.

The Dutch police records show that hackers share many similarities with other criminal suspects. The percentage of hacking suspects who are men does not differ significantly from the corresponding percentage of suspects of other crimes (Prins, 2008). Hacking, like other offline crimes, is usually committed by people who are less than 45 years of age. Hackers tend therefore, like offline criminal suspects, to be younger than average for the Dutch population.

While e-fraudsters are relatively young, e-fraud is not generally committed by those in the youngest age group (12-17). Suspects of e-fraud are mainly found in the category 18-34 years (78.9%). One possible explanation is that those in the youngest group (12-17 years) do not have the social skills to commit e-fraud. Contrary to hackers, e-fraud suspects need to have manipulative skills in order to scam people.

Policing cyber crime in the Netherlands

This section is based on the study of Leukfeldt et al (2013) into the functioning of the Dutch criminal justice system regarding cyber crime. The police are responsible for detecting and investigating crime. In the Netherlands, so-called basic police units, as far as investigations are concerned, fight everyday crime. With the advent of cyberspace, the fight against cyber crime, such as fraud via the Internet, is now also part of the basic units' workload. These units consist of police employees without specialist knowledge of cyber crime. The research results presented here refer to basic police units that have to deal with everyday (cyber) crime cases.[11]

A first problem in detecting and investigating cyber crime lies in the fact that victims of cyber crime do not always notice that they are being victimized. In addition, a recent self-report study in the Netherlands shows that merely 13.4% of the victims report cyber crime to the police (Domenie et al., 2013). Subsequently, if victims do report cyber crime to the police, it is unsure whether the police will register the report. Interviews and earlier research suggest that police employees who are responsible for registration – which forms the basis of the criminal investigation process – have a lack of knowledge about cyber crime. As a result, they sometimes do not register cyber crimes and if they do, they are unable to register these offenses properly (Toutenhoofd et al., 2009). Thus, a first bottleneck in the fight against cyber crime is the fact that a significant part of cyber crimes will never enter the criminal justice system.

Once a crime has been registered, a screening process starts. A so-called case screener of the police checks to what extent the report includes keystones for criminal investigation. In the interviews, respondents repeatedly state that police reports about cyber crime cases lack such keystones, because of the deficit in knowledge of police employees in the registration process. As a result, these cyber crime cases will not lead to further investigation and flow out of the criminal justice process early.

Cyber crime cases that pass the screening are sent to teams of criminal investigators (not being cyber crime specialists). Due to scarce capacity, criminal investigators cannot handle all incoming cases. Therefore, the work offered to them is prioritized. Despite the fact that the Dutch government gives priority to cyber crime, criminal investigators consider cyber

[11] The Dutch Police Force does have 'digital experts'. However, in practice these experts are not involved in everyday crime investigations. They support severe criminal investigations (e.g. murder). Furthermore, The Dutch National Police Force has a Team High Tech Crime (THTC). This team is merely engaged in the fight against severe, organized and innovative forms of high impact cyber crimes on an (inter)national level.

cases as inferior to 'traditional' crimes. Respondents state that three main reasons underlie this observation: (1) the (social) impact of cyber crime is lower than the impact of traditional crime; (2) criminal investigators have a lack of *experience* regarding cyber crimes and (3) they have too little *knowledge* to effectively investigate these cases. The by definition scarce amount of criminal investigators therefore prefer to handle traditional crimes. The unwanted consequence is that cyber crime cases are not investigated, not prosecuted and thus not adjudicated.

The result of the quantitative analyses – following the reported cyber-cases – confirms the aforementioned findings. The police relatively often do not investigate cases of hacking and e-fraud. 80 per cent of the hacking cases and 46.4 per cent of the e-fraud cases were closed by the police, for example because of a lack of evidence, and thus never reached the prosecution process. Merely 5.9 per cent of the hacking reports and 18 per cent of the E-fraud cases were sent to the prosecution service. The way the remaining hacking (14.1%) and e-fraud reports (35.5 percent) were handled is unknown, because these reports could not be traced in the police registration system. In fraud cases, this is (partly) due to the fact that a significant proportion (26%) of the files is sent on to another local police force and is subsequently untraceable. For hacking cases, the reason for this is unknown. That e-fraud and hacking cases are generally handled by the police in this way, as respondents emphasised, is presumably due to a lack of priority and capacity when it comes to sufficient expertise in cyber crime to be able to handle these cases.

Implications for police policy

Cyber crime is about ordinary people

The study of police files shows that cyber crimes are often small, relatively simple offenses committed by more or less small-time offenders who work alone. Based on the file study it therefore seems plausible to assume that cyber crime has the same structure as conventional (offline) crime. Indeed, in conventional crime there is also a large group of offenders that commit relatively minor offenses (such as theft and burglary) on a more or less individual basis. Organized groups do not seem to have the monopoly on cyber crime. The average cyber criminal in the Dutch police files is not part of an organized gang of whiz kids who are able to do complex things with a computer. As with ordinary crime suspects, they are mostly men under 45 years, and, like in common crime, there are also female suspects and suspects from other age groups.

It is perhaps easier to imagine that e-fraud crimes are 'of the common people' than it is to imagine that hacking is. Hackers are perceived to be highly technically literate. But according to our study, hacking is now an offense which is within reach of many people. The fact that hacking is becoming more commonplace is probably related to the degree to which people in our society use and have become familiar with the virtual world. For young people who grew up with cyberspace ('digital natives') messing with someone else's account or profile is not necessarily a technical feat, but just a way to get at them.

Implication 1: The police have to deal with cyber crime more often and throughout their organization

The conclusion that cyber crime is about ordinary people has implications for the police. It means that handling cyber crime should not be reserved to specialized national teams of cyber experts (as has been the case traditionally). Instead, cyber-cases have to be treated by basic police units. Knowledge and skills about cyber crime should thus exist throughout the police force: every police officer should at least have some basic knowledge about cyber crime and how to settle everyday cyber cases. Police officers not only come into contact with isolated cyber crime cases, but with a variety of connections between offline and online crime. Increasingly police officers have to deal with a cyber aspect in traditional cases, for example, someone who is being stalked and whose e-mail account is hacked. New generations, who grow up in an era where computers and the Internet are indispensable, will increasingly have to deal with cyber crimes and traditional crimes such as threats and slander with a cyber element. Consequently, the police in the full breadth of the organization have to be able to deal with cyber crimes.

Implication 2: Hacking and e-fraud are internationalizing everyday police work

Almost a quarter of the hacking suspects, and almost fifteen per cent of the e-fraud suspects, operate from abroad. This is not surprising; in the literature cyber crime is also regarded a global problem (e.g., Europol, 2003; Jewkes & Yar, 2008; Van der Hulst & Neve, 2008). The global nature of the Internet has made it easy for offenders to cross the border and makes victims abroad. The workload of the police will become more international.

Traditionally, offenders who operate internationally are usually part of an organized group, for example, drug smugglers. Specialist police teams would be set up to deal with these groups. Small-time cyber criminals are now also cooperating internationally. An example of this would be an Englishmen scamming a Dutchman on an online auction site: everyday police work is being internationalized. Non-specialist teams in all police districts, who have no experience with international crime, will now also have to deal with cross border cases. In order to tackle these cyber crime problems, the police organization will have to adapt to this new situation.

Still, in the largest part of hacking and e-fraud cases, the perpetrator operates from within the country (see also Jansen, Junger, Montoya & Hartel, forthcoming). This means that, in addition to the above, the police should also have a strategy with respect to cyber crime from within the borders of the country.

Implication 3: the current organization of the Dutch police causes cyber-cases to never enter the criminal justice system or to flow out of the criminal justice process early.

Several problems hamper the effectiveness of the police in the fight against crime in the digital era. Basic police units, as far as investigations are concerned, have to fight common crime, including cyber crime. However, capacity within these units is scarce and the available police employees lack knowledge of, and experience with, cyber crime cases. In addition, the police consider the impact of cyber cases as inferior to the impact of traditional cases. This lack of (perceived) priority and proper capacity to fight digital crimes causes cyber cases to never enter the criminal justice system or to flow out of the criminal justice process early.

It is justifiable that crimes with a higher impact than cyber crime, such as murder or violent crime are given priority by the police. However, it is unjust when cyber cases are considered inferior to traditional cases just because of a lack of knowledge. As was already mentioned, it is thus evident that knowledge about cyber crime should be available right across the organization.

Enhancing cyber knowledge within the police should not be done by obligating police employees to handle cyber cases that, due to their low social impact, normally would not receive priority. After all, police capacity is scarce and should be used as efficient as possible. Instead, it seems worthwhile to enhance the cyber knowledge of police officers by making them handle the digital aspects of (traditional) high impact - and prioritized cases. In everyday police practice that, for example, means that a criminal investigator who is involved in handling a violent crime, is given the task to also conduct research on the computer of the suspect in order to (if plausible) find out about possible online threats that preceded the violent crime. This approach aims to show police employees that digital information can enrich - and should thus standard be incorporated in - criminal investigations. Furthermore, this approach is supposed to enhance cyber-knowledge and reduce 'cold feet' with regard to handling cyber cases.

Finally, it has to be noted that a current police priority is to improve the capabilities of regional teams to combat cyber crime. Several initiatives, such as the development of an e-learning course about cyber crime and a guide to register reported cyber crimes, aim to enable the Dutch police to effectively handle cyber crime throughout the organization (Stol, Leukfeldt & Klap, 2012).

References

Algemene Rekenkamer (2012). *Prestaties in de strafrechtketen.* [Performances of the criminal justice system]. Den Haag: Sdu Uitgevers.

Bernaards, F., E., Monsma., & Zinn, P. (2012). *High Tech Crime. Criminaliteitsbeeldanalyse 2012.* Rotterdam: Theme Media Center.

Campman, I. P., Dedert, R., Hesseling, P. J., Huijskes, D., Kegel, N., Tijsmans, S., & van Vulpen en Z. Witteveen (2012) *Criminaliteit in een gedigitaliseerde samenleving.* [Crime in a digitalized society] Amsterdam: Regiopolitie Amsterdam-Amstelland.

CBS (2012) ICT, kennis en economie 2012. [ICT and the economy 2012] Den Haag/Heerlen: Centraal Bureau voor de Statistiek.

Cozijnsen, A. J. (1989) *Het innovatievermogen van politie-organizaties.* [Innovation Capacity of Police Organizations] Deventer: Kluwer Bedrijfswetenschappen.

Bunt, H. G., van de., & Kleemans, E. R. (2007) *Georganiseerde criminaliteit in Nederland, derde rapportage op basis van de Monitor Georganiseerde Criminaliteit.* [Organized Crime Monitor of the Netherlands] Den Haag: WODC.

Dijkstra, J. J. (2008). Computercriminaliteit. In C. W. J. de Vey Mestdagh, J. J. Dijkstra & S.C. Huisjes (ed.), *ICT-recht. Voor de praktijk.* [ICT and Law] Groningen: Wolters Noordhof.

Domenie, M. M. L., Leukfeldt, E. R., van Wilsem, J. A., Jansen, J. & Stol, W.Ph. (2013) *Victimisation in a digitized society: A survey among members of the public into e-fraud, hacking and other high volume crimes.* The Hague: Eleven International Publishers.

Domenie, M. M. L., Leukfeldt, E. R., Toutenhoofd-Visser en, M. H., Stol, W. Ph. (2009). *Werkaanbod cyber crime bij de politie. Een verkennend onderzoek naar de omvang van het geregistreerde werkaanbod cyber crime.* [Registered cyber crimes by the police in the Neherlands] Leeuwarden: NHL.

Europol (2003). *Computer-related crimes within the EU: Old crimes new tools, new crimes new tools.* Luxemburg: Office for Official Publications of the European Communities.

Grusky, O. en., & Miller A. A. (1981). *The sociology of organizations. Basic studies.* New York: The Free Press.

Helmus, S., Smulders, A., & Zee, F. van der. (2006). *ICT Veiligheidsbeleid in Nederland – Analyse en overwegingen bij Herijking.* [ICT Safety and Security Police in the Netherlands] TNO: www.tno.nl (ongerubriceerd), nr. 035.31231.

Jansen, J., Junger, M., Montoya, L. & Hartel, P. (forthcoming) Offenders in a digitized society. In W.Ph. Stol & J. Jansen, (Eds) *Cyber crime and The Police*, The Hague: Eleven International Publishers.

Jewkes, Y., & Yar, M. (2008). Policing cyber crime: emerging trends and future challenges. In: T. Newburn (Ed). *Handbook of policing* (580-607). Cullumpton: Willan.

Kleemans, E. R., Brienen, M. E. I., van de Bunt, H. G., Kouwenberg, R. F., Paulides, G., & Barensen, J. (2002). *Georganiseerde criminaliteit in Nederland, tweede rapportage op basis van de WODC-monitor.* [Organized Crime in the Netherlands, second report] Den Haag: WODC.

KLPD (2004). *Nationaal dreigingsbeeld zware of georganiseerde criminaliteit: een eerste Proeve.* [National Report on Organized Crime] Zoetermeer: Dienst Nationale Recherche Informatie.

KLPD (2007). *Cyber crime - Focus op High Tech Crime: Deelrapport Criminaliteitsbeeld 2007.* [Cyber crime: Focus on high tech crime] Rotterdam: Theme Media Center.

KNAW (Koninklijke Nederlandse Akademie van Wetenschappen) (2003). Gedragscode voor gebruik van persoonsgegevens in wetenschappelijk onderzoek. Advies van de Sociaal-Wetenschappelijke Raad. [Code of conduct for social scientific research] Amsterdam: KNAW.

Lammers, C. J. (1983). *Organizaties vergelijkenderwijs.* [Organizations] Utrecht/Antwerpen: Het Spectrum.

Leertouwer, E. C. & en S.N. Kalidien (2011). De strafrechtketen in samenhang, in: Kalidien, S.N. & N.E. de Heer-de Lange (red) *Criminaliteit en rechtshandhaving 2010. Ontwikkelingen en samenhangen.* [Crime and law enforcement 2010: developments and correlations]. Den Haag: WODC.

Leukfeldt, E. R., Veenstra, S. Domenie, M. M. L., and Stol, W. Ph. (2013). *De strafrechtketen in een gedigitaliseerde samenleving: een onderzoek naar de strafrechtelijke afhandeling van cyber crime.* [The criminal justice system in the digital era: a study on the way the criminal justice system handles cyber crime]. Leeuwarden: NHL Hogeschool, Lectoraat Cybersafety.

Leukfeldt, E. R., Kentgens, A., Frans, B., Toutenhoofd, M., Stol, W.Ph. & Stamhuis, E. (2012). Alledaags politiewerk in een gedigitaliseerde wereld. Handreiking voor delicten met een digitale component. [Handbook of crimes with a digital component] Den Haag: Boom Lemma Uitgevers.

Leukfeldt, E. R., Domenie, M. M. L. & Stol, W.Ph. (2010). Verkenning Cyber crime in Nederland 2009. [Cyber crime in the Netherlands 2009] Den Haag: Boom Juridische Uitgevers.

PAC (2008). *Programmaplan. Programma Aanpak Cyber crime*. [Program Plan. Program Against Cyber crime] De Bilt: interne notitie.

Pfeffer, J. (1982) *Organizations and organization theory*. Marshfield (Massachusetts): Pitman Publishing Inc.

Prins, L. (2008). *Landelijke Criminaliteitskaart. Populatieprofielen 2007.* [National Crime Picture 2007] Zoetermeer/Driebergen: KLPD.

Sackers, H. J. B., & Mevis P. A. M. (eds). (2000). *Fraudedelicten*. [Fraud] Deventer: W.E.J. Tjeenk Willink.

Stol, W. Ph., Leukfeldt, E. R. & Domenie, M. M. L. (2011). Internet, Crime and the Police. *Journal of Police Studies*, *20*(3), 59-81.

Stol, W.Ph. (2008). Cyber crime [Cyber crime], In: W. Ph. Stol en & A. Ph. Van Wijk (red.) *Inleiding criminaliteit en opsporing*. Den Haag: Boom Juridische Uitgevers.

Stol, W. Ph., Leukfeldt, E. R., & Klap, H. (2012). Cyber crime en politie: een schets van de Nederlandse situatie anno 2012 [Cyber crime and police: a draft of the Dutch Situation in 2012]. *Justitiële Verkenningen* 38 (1).

Toutenhoofd-Visser, M.H., Veenstra, S., Domenie, M. M. L., Leukfeldt, E. R., & Stol W. Ph. (2009). *Intake en Eerste Opvolging. Een onderzoek naar de intake van het werkaanbod cyber crime door de politie*. [Intake and first response of cyber crimes] Leeuwarden: NHL.

Van der Hulst, R. C., & Neve, R. J. M. (2008). *High-tech crime: inventarisatie van literatuur over soorten criminaliteit en hun daders*. [High Tech Crime. Literature review about crimes and their offenders] Den Haag: WODC.

Vijver, C. D. van der, & en Terpstra, J. B. (2007). 'Organisatie en sturing van politiewerk' [Organization of police work] in Fijnaut, C.J.C.F., Muller, E.R., Rosenthal, U. en E.J. van der Torre (eds) *Politie: studies over haar werking en organizatie*, Deventer: Kluwer.