VU VRIJE UNIVERSITEIT AMSTERDAM

VU Research Portal

Criminals seeking ICT-expertise

Bijlenga, Nadine; Kleemans, Edward R.

published in
European Journal on Criminal Policy and Research
2018

DOI (link to publisher)
10.1007/s10610-017-9356-z

document version
Publisher's PDF, also known as Version of record

document license
Article 25fa Dutch Copyright Act

Link to publication in VU Research Portal

citation for published version (APA)
Bijlenga, N., & Kleemans, E. R. (2018). Criminals seeking ICT-expertise: an exploratory study of Dutch cases. *European Journal on Criminal Policy and Research*, *24*(3), 253-268. https://doi.org/10.1007/s10610-017-9356-z

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal

Take down policy
If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

E-mail address:
vuresearchportal.ub@vu.nl

Download date: 28. Apr. 2025

Eur J Crim Policy Res (2018) 24:253–268
DOI 10.1007/s10610-017-9356-z

Criminals seeking ICT-expertise: an exploratory study of Dutch cases

Nadine Bijlenga[1] · **Edward R. Kleemans**[1]

Published online: 22 August 2017
© Springer Science+Business Media B.V. 2017

Abstract Which opportunities due to digitization are exploited by criminals? And how do criminals gather the required ICT-expertise to take advantage of these opportunities? This exploratory study provides insight into criminals seeking ICT-expertise by analyzing five Dutch cases. This paper shows that criminals seeking ICT-expertise take advantage of companies and employees in the ICT-sector that act in a gray area. It is noteworthy that the initial contact of criminals seeking ICT-expertise is often immediately directed to criminal collaboration. In these cases, 'capacity' is more important than 'contact'. Furthermore, this paper discusses the role of forums for criminals seeking ICT-expertise. Criminals take advantage of the transfer of knowledge on forums and the existence of crimeware-as-a-service. Finally, this study falsifies the statement that there is a clear division between traditional offender groups taking advantage of the possibilities arising from ICT, and crime groups operating exclusively online. In practice, there are many connections between online and offline activities.

Keywords Cybercrime · Online forums · ICT-specialists · Criminal careers · Recruitment

Introduction

Criminals have a keen eye for discovering new opportunities and then take advantage of them (Williams 2001). Digitization offers both opportunities for the emergence of new types of crimes, and for the enhancement of traditional crimes (e.g., Holt and Bossler 2014; McGuire

In collaboration with Team High Tech Crime (THTC) of the Dutch police.

✉ Nadine Bijlenga
nbijlenga@gmail.com

Edward R. Kleemans
e.r.kleemans@vu.nl

[1] Faculty of Law, VU University Amsterdam, De Boelelaan 1105 1081 HV, Amsterdam, The Netherlands

and Dowling 2013). Consequently, a broad spectrum of crimes appears in which ICT plays a role. Cybercrime is used as an umbrella term for both cyber-dependent and cyber-enabled crimes. Although it is clear that ICT provides new possibilities for criminals, very little is known about criminals seeking ICT-expertise (for an overview, e.g., Wall 2007; Holt and Bossler 2014; Lavorgna 2015a).

Choo (2008) states that there are two types of groups taking advantage of the possibilities arising from ICT. On the one hand, traditional organized offender groups; on the other hand, organized cybercrime groups who exclusively operate online. He argues that it is important to keep in mind that there is a big distinction between these groups because they operate from a different perspective. Conversely, in this paper, we pose the question if and how these groups are intertwined. Furthermore, this study explores how and where criminals acquire ICT-expertise to commit crimes.

The theoretical framework of this paper combines opportunity theory (Clarke and Felson 1993), social network theory, and ideas about offender convergence settings (Felson 2003). Clarke and Felson (1993) state that criminality should be interpreted as a normal social phenomenon, and criminals should be viewed as individuals reacting to circumstances and opportunities. Consequently, the focus of this paper is on the opportunities arising from ICT, rather than on the specific technical means used. After all, every technical development could be understood as an opportunity for criminal activity, either as a target or as a means to an end (Zittrain 2006, p. 2021).

This paper provides insight into criminals seeking ICT-expertise through an exploratory analysis of five Dutch criminal investigations. Moreover, this paper highlights criminals taking advantage of companies and employees in the ICT-sector that act in a gray area, and discusses the role of forums for criminals seeking ICT-expertise. The next section gives a brief overview of the theoretical framework, followed by data and methods. Then the main empirical results are elaborated upon. Finally, the main conclusions and implications for policy are discussed.

Theoretical framework

Exploiting opportunities

Which opportunities are exploited by criminals? Former research describes various examples of criminals using technologies for criminal purposes. It is stated that anonymity is one of the most important characteristics of crimes perpetrated in cyberspace (Longe et al. 2009). In sub-Saharan Africa, many fraudsters have already migrated from the streets to the internet, because the internet provides better chances to remain anonymous (Longe et al. 2009). Additionally, Western individuals and loosely organized criminal networks have been exploiting online opportunities to create criminal markets (e.g., Lavorgna 2015b; Zabyelina 2017). Furthermore, the internet might facilitate organized crime, and it is stated that a dynamic relationship exists between online and offline organized crime (see e.g., Europol 2014, 2016). Nevertheless, it is not clear to what extent organized crime groups exploit these opportunities.

Lavorgna and Sergi (2014) state that mafia-style groups operating in non-traditional territories embrace online opportunities. Furthermore, business-like groups use the internet as an enhanced communication tool, because it enhances efficiency and lowers risks. Terrorist groups, such as Al Qaida, have used encryption to reduce the value of electronic intercepts, and have made low-tech adjustments in communication. They use the internet to recruit and

train supporters, and the internet is increasingly used to plan and coordinate terrorist operations (Kenney 2007).

Nevertheless, mafia-style groups are reluctant to use the internet, because they do not feel the need to change, and because persons with higher positions in the hierarchy are hardly ever digitally native (Lavorgna 2015a). Therefore, mafia-style groups use the internet merely as a communication tool to avoid wiretapping.

Seeking ICT-expertise

How do criminals gather the required ICT-expertise to exploit opportunities? The literature indicates that personality traits only affect the ability of a person to commit cybercrimes to a limited extent, because criminal collaborations and ready-to-use tools and services enable criminals to commit cybercrimes (Holt et al. 2012; Odinot et al. 2016; Sood and Enbody 2013). Criminals who seek ICT-expertise can either develop the required ICT-skills themselves or establish collaboration with someone with ICT-expertise.

Establishing collaborations

For the establishment of successful collaborations, both 'contact' and 'capacity' are important (Van de Bunt and Kleemans 2007). For new criminal collaboration, people from one's own network are preferred, due to the risk of being arrested and the risk of betrayal (Reuter 1983). Bruinsma and Bernasco (2002, p. 138) argue that trust is more important when criminal activities are riskier. One of the problems of criminal networks, however, is that existing social ties are often highly clustered, which is why sometimes outsiders with specific capacities are necessary for certain roles (Kruisbergen et al. 2012). Therefore, weak ties are essential for establishing opportunities and can be thought of as a bridge between different groups (Granovetter 1973).

As 'capacity' and certain ICT-skills might be lacking in traditional criminal networks, existing contacts might be less relevant than more risky ways to liaise with ICT-'capacity'. How can such collaborations emerge? Kleemans and Van de Bunt (1999) challenged the traditional view on recruitment by introducing the idea of the social snowball effect, by which people get involved in criminal activities through their social relations and gradually evolve from there until they choose their own ways. Kleemans and De Poot (2008) describe five mechanisms by which starters get involved in organized crime: existing social contacts, work, sidelines and leisure activities, negative life events, and deliberate recruitment. These mechanisms could also be used to study how collaborations are established between criminals and persons with the required ICT-expertise. A mixture of rewards and threats could ensure that ICT-specialists carry out criminal tasks effectively and efficiently, so that criminals do not have to develop technical skills themselves (Williams 2001).

Felson (2003, 2006) coined the term 'offender convergence settings'. These settings provide opportunities for criminals to establish new contacts outside their initial social network. Starting out with physical offender convergence settings, such as the 'rough bar', this idea can also be extended to virtual offender convergence settings. In particular, forums and websites with encrypted access provide opportunities for establishing new criminal contacts. In addition, Brenner (2001) describes a virtual world, called cyberspace, existing alongside the physical world. These virtual offender convergence settings provide starters with

easy access to criminals (e.g., Lu et al. 2010; Soudijn and Monsma 2012). Moreover, in order to access certain forums, potential members are screened and have to prove that they are active cybercriminals (Ablon et al. 2014; Holt et al. 2015; Lusthaus 2012; Soudijn and Zegers 2012; Yip et al. 2013).

Forums are used particularly to recruit specialists and offer a place where co-offenders can meet, recruit, and trade criminal 'services' (Leukfeldt et al. 2017b, 2017c). Forums and online markets are a very important focus of new empirical research (see e.g., Holt and Lampke 2009; Soudijn and Zegers 2012; Décary-Hétu and Dupont 2012; Yip et al. 2012; Martin 2014; Dupont et al. 2016).

Even though virtual offender convergence settings are becoming more important, Leukfeldt (2014) shows that contacts between phishing offenders are established through physical offender convergence settings instead of virtual ones. In addition, existing social ties still play an important role in cybercriminal networks. Therefore, both online and offline contacts seem to be important (Holt 2007; Holt and Bossler 2014; Leukfeldt et al. 2017a).

Enabled and facilitated cybercrimes

Another development is that crimeware is available on request and, as a result, could easily be used by criminals with limited technical expertise (Sood and Enbody 2013). Therefore, criminals can gain the required ICT-expertise themselves and are not dependent on establishing criminal collaborations. In addition, Leukfeldt et al. (2017a, b) state that in criminal groups engaging in financial cybercrime (through phishing and hacking) only a few offenders have high technical expertise. Subsequently, online forums provide specific information about how to commit offenses, which is why cybercrimes are enabled and facilitated by unknown persons, and therefore criminals can gain the developed knowledge without establishing a close criminal collaboration (Hutchings and Holt 2015; Hutchings 2014; Leukfeldt et al. 2017b; Soudijn and Zegers 2012). Additionally, many forums have rating systems, so trust is established in the data, tools, and services for sale (Ablon et al. 2014; Dupont et al. 2016; Decary-Hétu and Dupont 2012; Holt et al. 2015; Lusthaus 2012; Soudijn and Zegers 2012; Yip et al. 2013).

Data and methods

Case inventory

Five Dutch criminal investigations were analyzed in order to gain insight into criminals seeking ICT-expertise. In order to collect a broad variety of cases, various cybercrime cases with an offline aspect were collected. As in many other countries, the Netherlands lacks a central registration system that would allow for a quick overview of all criminal investigations, including information to make relevant selections of cases. Therefore, the selection of cases was made by using the snowball method.

The search for relevant cases started at the national Team High Tech Crime (THTC) of the Dutch police. Through the attendance of team meetings, and being physically present in the investigation team during the research period (2015-2016), the first author gained insight into various cybercrime cases under investigation. The main focus of this team is combatting high-

tech crime. Crimes are labeled as high-tech crime, if ICT is used as a target, if innovative ICT is used, if there is intermingling between the licit and the illicit world, or if the crime has great social impact (Bernaards et al. 2012). Therefore, these cases can be interpreted as a specific subset of all cybercrime cases. People from this team were asked whether they knew investigations in which cybercriminals played a role in traditional offender groups.

The search for relevant cases continued by approaching digital expertise teams of the ten Dutch police districts by email and telephone. These digital expertise teams provide digital support in complicated criminal investigations. People involved in those teams were asked whether they knew investigations in which ICT-specialists played a role in traditional offender groups. Hence, we tried to capture high-tech crime cases with relationships with traditional crime groups on the one hand, and traditional cases connected to cybercrime specialists on the other hand. Through this two-way approach, we studied not only more 'traditional' cybercrime cases, but also cases involving offenders who do not meet the traditional standards of a cybercriminal. During this inventory period (2015-2016), people from both types of teams were also asked whether they knew other people who could bring up relevant cases. As a result, more people from different specialized teams of the Dutch police have been approached.

Case selection

After the collection of cases, a purposive sample of five cases has been selected (Glaser and Strauss 1967). These cases have been analyzed in-depth. The most important selection criterion was the relevance of the case for the purpose of this research (George and Bennett 2005, p. 83). The purpose of this research is to gain insight into criminals seeking ICT-expertise. For this purpose, information about the modus operandi in general and specific information about collaboration is important.

First, cases were selected on the basis of the quality of the data and the amount of available information about the modus operandi and the collaboration. Second, cases were selected that could provide a broad picture of the various ways in which ICT might play a role in crime. Accordingly, a heterogenic sample of cases was formed with well-known and less well-known types of crime in which ICT plays a role.

The selected cases comprise drug trafficking, encryption, a contract killing, illegal online markets, and banking fraud. In three out of five selected cases, the suspect has been convicted. In the other cases, there has not been a court ruling yet, but the description of the modus operandi itself is clear. In the analysis of these cases, the focus is on the modus operandi and not on the suspect. In both cases, the information about the modus operandi is clear.

The strength of this study is to empirically explore the various ways in which criminals make use of possibilities that arise from ICT. Therefore, different cases have been selected, and heterogeneity is more important than the common factor of these cases. Furthermore, this is an exploratory in-depth analysis with a small sample size. This is why it is important to be careful with generalizing the results to other cases. We will revisit this issue in the last section.

Analytical framework

The five cases have been collected in order to verify, falsify, or specify previous findings of research. This was done in accordance with the concept of theoretical sampling (Glaser and Strauss 1967). The cases were analyzed by investigating police files, conducting formal and

informal interviews, and attending two court trials. A standardized list of topics was used to describe all cases. In this way, the information was collected in a structured and systematic way (see Appendix 1).

The cases were first analyzed by studying the police files, creating a detailed picture of the daily, social life of the suspects. At the same time, the police files were used to verify statements made by police officers in interviews and to get a closer look into aspects mentioned by police officers. The Dutch police files provide unique insight into the studied collaborations due to extensive use of special investigative methods, such as wiretaps, observations, undercover policing, and house searches. It should be noted that information gathered by the Dutch police, in general, provides useful information for researchers. This is, in particular, the case because of the absence of plea-bargaining in the Dutch criminal justice system and unobtrusive police methods, such as wiretapping and IP-taps, which were used and the results of which can be checked by researchers themselves (see Kleemans 2014). Finally, the police files contained background information on the technical resources used. This offers the researcher information to fully comprehend the role of ICT in the modus operandi. Nonetheless, it should be taken into account that information in police files is primarily collected to gather enough evidence against the suspect, as opposed to collecting information primarily for the purpose of scientific research. As a result, most information is gathered regarding those persons in an offender group who are actually prosecuted by the police, and accordingly, less information is available about other people. This is why a fragmented picture of an offender group may arise. In particular, information about the first encounter between two suspects may remain unknown. Detailed information about criminal associates abroad may remain unknown as well. However, in some cases, information derived from forums is gathered and the physical location of the associate plays a smaller role. Finally, some information in the police files might have poor internal validity, such as possible false statements during interrogations. Therefore, this research is mostly based on information gathered by unobtrusive methods such as wiretaps and IP-taps.

In addition, formal and informal interviews have been conducted. The formal interviews, following the model of a semi-open interview, were conducted with police team managers and police officers who are responsible for the police files. The standardized list was used as a starting point for conducting the interviews, to collect this information in a structured way. Finally, it was possible to attend two trials in one of the studied cases, which made it possible to take this into account while researching this case.

Empirical results

Seeking ICT-expertise

Which level of ICT-expertise was required to take advantage of specific opportunities? And how did the criminals gather the required ICT-expertise to take advantage of specific opportunities? In general, criminals can gain the required ICT-expertise by establishing criminal collaborations, or by using ready-to-use tools and services. On the basis of previous research into organized crime, it would be expected that collaborations are established through social ties, work relationships, leisure activities and sidelines, through life events, or deliberate recruitment. This subsection looks into mechanisms by which collaborations are established in order to gather the required ICT-expertise to take advantage of specific opportunities.

Case descriptions

Case 1 The first case involves offenders engaged in the transport of drugs, as well as in spy shops. They try to find a method to get illegal goods out of containers in the harbor. The illegal drugs have been put into these containers in drug producing countries, and it is essential to obtain these drugs before the container is picked up by the licit transport company. For this reason, physical key loggers are placed, and also targeted phishing emails are sent, resulting in malware infection of computers of port authorities. Consequently, the offenders are able to watch at which time specific containers enter the harbor, and they are also able to intercept the pin codes by which the containers can be picked up. In this case, the offender is looking for a specific person who can help with these criminal activities.

In the past 1A has done business with an employee of a security company, 1B. When they are finishing up their business affairs, 1B mentions that he is developing an application and is looking for investors. 1A offers to invest in this project if 1B would show him his capabilities. Their criminal collaboration starts to evolve at this very moment. However, the first activities are not obviously criminal. The activities to which 1B contributes are gradually directed at drugs trafficking.

This case shows that both parties get into contact with each other because of a work relationship. The collaboration does not immediately start on a criminal basis, and it is difficult to determine whether or not the ICT-specialist is realizing what exactly he is getting into. Furthermore, in defense, this ICT-specialist stated that he had been coerced, and it is difficult to determine whether or not, and to what extent this really is the case.

After a while, other ICT-specialists are also asked to help with the technical aspects of trafficking drugs into the port.

Because of the expertise level required for the task, 1B asks two friends to help. Therefore, two other ICT-specialists, 1C and 1D, get involved in drug trafficking activities. 1B came into contact with 1C and 1D through a hacker society in which they were involved when they were younger. At this moment, they are all in their thirties, and all have their own specialization.

This case contains a targeted attack in which advanced technical means are used. The process of a targeted attack is more intensive than an untargeted attack. This is the case because vulnerabilities of one specific system need to be sought, instead of vulnerabilities of a random system. In this case, they adapted legal software, through which they could eventually install malware automatically on computers. This is why, in this case, a high level of expertise is needed to fulfill the task successfully. The involved ICT-specialists are highly educated and are working in the ICT-sector.

Case 2 The second case concerns encrypted communication between multiple offenders. ICT does not play a role in the modus operandi itself, but ICT is used to shield activities against the authorities. The ICT-specialists run a company through which they offer encrypted communication to criminals. They have closed systems in which communication is only possible if phones from that particular company are used. Consequently, the traditional criminals do not

need to have knowledge about ICT, because they are able to outsource this task to a company.

2A and 2B get into contact with a company offering equipment to shield their communication against the authorities. This company provides equipment, without storing information of the customers. Because this equipment is not considered illegal in the Netherlands, this company is easily found, and is well-known in the criminal circuit.

This case shows that offenders can easily find the right equipment and services through a company that is easy to approach because encrypted communication is not illegal in the Netherlands. Even though the technics behind encryption are advanced, the company selling these encrypted mobile phones can make use of existing methods. The initial contact is easily made, and the contact is immediately directed by supply and demand. Nevertheless, criminals value their anonymity, and therefore they choose a company that does not store information of the customers. Furthermore, the criminals trust this company, because it is well-known in the criminal circuit.

Case 3 The third case concerns a contract killing in which spyware is used. The offenders are searching for information to determine the 'chokepoint' for a contract killing. That is why spyware is secretly put on the mobile phone of the victim. Shortly before the contract killing, the offenders give the victim a new mobile phone that has been completely encrypted. The victim does not know that spyware has been put on this mobile phone, through which his opponents have access to his location and microphone. This way, his opponents are able to get a clear picture of his daily routines and are able to decide on a suitable 'chokepoint' for the contract killing. Technical skills are needed to adapt the software for a specific purpose, and to make it ready to use.

3A and 3B want to have information to determine the chokepoint for the contract killing. Therefore, they get into contact with a company offering spyware equipment, and that is able to put this software on the mobile phone. Because this equipment is not considered illegal in the Netherlands, this company is easily found, and is well-known in the criminal circuit.

Similar to the second case, the initial contact is easily made, because the software in itself is not illegal. The contact is also directed by the supply and demand of both parties. In the Netherlands, the personal data protection act prescribes that personal data may only be processed if the subject has unambiguously given consent. Therefore, in this case, the technology is used for illegal purposes. The company itself acts in a gray area because providing spyware is not illegal in itself, but customers often use spyware for illegal purposes. In this case providing these services involves more risks than in the second case, which is why trust presumably plays a bigger role. Furthermore, the offenders, in this case, have the control over the control panel themselves. Therefore, the offenders need to have some technical skills.

Case 4 In the fourth case, ICT is particularly used as a communication tool. The offender, who could be described as a normal family man, offers and sells drugs on a daily basis. He works together with drug suppliers he either approaches or who approach him. He sells drugs on illegal online markets that can only be entered by using the TOR network, and where customers pay for their drugs in Bitcoins, a virtual currency.

The offender gathered information about the use of TOR and paying with Bitcoins on the internet. This information is easy to access, and therefore people without much

knowledge about ICT can easily use it. Consequently, no collaboration is established to gain ICT-expertise about offering and selling drugs on illegal online markets. The offender had made a list of the steps he needed to take to use TOR.

Using an illegal online market does not differ much from the use of legal online markets. It can be concluded that even though a lot of the activities in this case take place online, and TOR and Bitcoins are used, only few technical skills are required.

Nevertheless, collaborations have been established online with other drug sellers to purchase large amounts of drugs. These collaborations often took place both online and offline, because drugs were transported between wholesalers, sellers, and buyers. They talked about drugs which are difficult to obtain, and they discussed where to find them. These collaborations were mostly controlled by supply and demand, which is why the first encounters were immediately directed at starting a criminal collaboration.

Furthermore, it is clear that a large number of potential partners is available on online markets. Gaining trust does not play an important role because of the anonymity in which they operate. Regarding the role of trust, the first contact does not necessarily lead to a long period of suspicion because the rating and reviews from every supplier are visible. It can be concluded that trust is mostly based on this online reputation and collaboration will be continued if prior experiences are good.

Case 5 The fifth case concerns four persons convicted for stealing from Dutch bank accounts. Some of these offenders have also been convicted for stealing in the physical world. They infected computers with malware. Consequently, persons trying to reach the website of their bank entered a manipulated website made by the offenders. When entering credentials on this website, these data were automatically saved and sent to the offenders. In addition, malware was put on the mobile phone of the victim, therefore the verification code could be intercepted. The initiator of this offender group was a Dutch college student. He got interested in banking fraud and contacted persons with knowledge about malware and managing botnets. The offender depended on the knowledge of more experienced persons, because he was still unexperienced. That is why he tried to get advice regarding specific aspects. For other purposes, he made use of crimeware-as-a-service. One of the collaborations started on Jabber:

5A gets into contact with 5B, someone living in Eastern Europe, on Jabber. Two days after their first encounter, 5A suggests to start cooperation. They discuss the possibilities of banking fraud in general, and stay in contact discussing the concrete details of their collaboration.

It can be concluded, that these partners met each other through a virtual offender convergence setting. These virtual offender convergence settings comprise many potential partners, and gaining trust seems to play an almost negligible role. In these meeting places, both parties try to hide their identity, and the first encounter is immediately focused on finding possibilities for criminal collaboration.

The next collaboration within this case involves a first encounter not immediately directed at criminal activities.

5A and 5C get to know each other by playing a virtual shooting game. After having virtual contact for a period of time, they start to meet in physical settings. Eventually, 5A gets involved in a criminal activity through which they can make big profits together.

This example shows that these partners first got to know each other before they started to collaborate in criminal activities. Compared to the earlier described role of 'capacity' and 'contact', the prominence of capacity and contact vary in this case. The first example shows the importance of capacity (searching for specific expertise), whereas the second example makes clear that virtual settings may also operate similarly to social settings in the physical world: first setting the scene for contact and increasing trust, which after a while may provide a fertile basis for criminal collaboration.

Main results: Seeking ICT-expertise

Five cases have been discussed in which criminals seek ICT-expertise. In four out of five cases collaborations were established to gather the required ICT-expertise. In the fourth case no collaboration was established, because information about the required ICT-expertise is easily accessible on the internet. Even though in the fifth case information was also easily accessible, collaborations were still established in order to gather more specialized ICT-expertise. The four other cases included six first encounters. Table 1 summarizes the characteristics of these first encounters: the mechanisms through which the first contact is established and whether or not the first encounter is immediately directed at criminal collaboration.

What is striking in this table is that a work or business relationship is the basis of the collaboration in three instances; subsequently, it is also worth noting that in these cases the most advanced technical equipment is used. Two of three of these first encounters were immediately directed at criminal collaboration. This is the case because, even though the companies did act in a gray area, the products provided in these cases were not illegal, which is why as a result gaining trust was of less importance. Furthermore, social ties and leisure activities and sidelines are the basis of collaboration. Finally, forums play an important role in the first encounter, and these encounters on (anonymous) forums are almost immediately focused on criminal activities. Moreover, these forums are also used to gather information without establishing a collaboration.

Table 1 shows that three out of six first encounters were immediately directed at criminal collaboration. In these cases, 'capacity' is more important than 'contact'. Regarding forums, the anonymity and illegal activities are important characteristics. Regarding the other encounters, the fact that the software and equipment in itself are not illegal provides the basis for this almost immediate focus on criminal activities, either by one party (ordering equipment for criminal activities) or by both parties (knowingly or unknowingly providing services and equipment for criminal purposes).

Table 1 The first encounter

Case	Mechanism	Immediately directed at criminal collaboration?
1	Work relationships	No
1	Social ties	No
2	Work relationships	Yes
3	Work relationships	Yes
4	-	-
5	Forums	Yes
5	(Online) leisure activities and sidelines	No

Interrelation between traditional offender groups and cybercrime

Choo (2008) states that there are two types of groups taking advantage of the possibilities arising from ICT. In this study, no clear division between those groups is recognized. At first sight, the first case looks like a perfect example of a traditional organized offender group taking advantage of the opportunities arising from ICT. This case concerns a traditional type of crime, e.g., importing drugs, as well as spy shops. The offenders of the traditional offender group have a financial motive for their activities, yet they do not differ much in that respect from the highly educated ICT-specialist. Both types of offenders can be understood as entrepreneurs constantly looking for ways to earn more money. The difference between those offenders is that the ways in which the ICT-specialist had earned money in the past were legal.

Additionally, it is also important to recognize that the traditional offenders in the first case do not form a secretive and closed group, but a network in which not everyone knows each other. The way in which these ICT-specialist are brought in is not so much different from the way in which other partners get involved. If somebody is needed for a specific bottleneck, they try to find somebody within their own network with specific capacities.

The third case, the contract killing case, also appears to be a good example of a traditional offender group making use of ICT. In this case, spyware is used to determine the chokepoint for a contract killing. In this case, it should be noted that the initial contact is established as a result of a weak contact. More in particular, this spyware can be easily ordered from a specific company.

In addition to these traditional offender groups, Choo (2008) states that there are also organized cybercrime groups operating exclusively online. The case which seems to be a good example of such a group at first sight, however, turns out to contain many elements of traditional crime. Moreover, in both the fourth and the fifth case, financial profits are of great importance, and the offenders are constantly trying to improve the modus operandi. Therefore, innovation should be considered as an inherent aspect of 'traditional crimes', which is why the clear distinction between traditional and cybercrime groups cannot be recognized in the studied sample. Additionally, money mules play an important role in the fifth case (see also Leukfeldt et al. 2017b, c). Money mules are also often used in traditional criminality for money laundering purposes. Therefore, the criminals in these crime groups do not only face similar problems as in traditional crime, but they also do not act exclusively online.

Furthermore, it is not clear if the fourth case should be classified as a traditional offender group, or as an exclusively online operating group. This is because the offenders are engaged in a traditional type of crime, drugs trade, even though a large part of the activities take place online. Even though in this case drugs are sold online, the drugs do have to be sent physically. Furthermore, the meetings between suppliers and sellers often take place physically. Therefore, there are both features of online organized crime groups, and of traditional offender groups.

This leads to the conclusion that, in practice, the differences between traditional offender groups making use of the possibilities of ICT, and crime groups operating exclusively online is not recognized in this study. Moreover, there are many connections between the online and the offline world, and between online and offline activities. This conclusion is in line with the conclusion by Leukfeldt et al. (2017a, b, c).

Conclusion and discussion

The focus in this paper on criminals seeking ICT-expertise generates some interesting empirical insights. The role of work relationships in the first encounter of more advanced cases is of interest for combatting crime. Work relationships could be the basis for collaboration in two different ways. Firstly, criminals use legal goods for illegal purposes, which is why they take advantage of licit companies. Furthermore, in these companies, a significant share of the customers are criminal. These companies, therefore, act in a gray zone.

Secondly, employees in the ICT-sector can be encountered in tasks for criminal purposes. This can also be viewed as a gray area, because at the start of a work relationship, the nature of the assignment is not always clear. In this way, ICT-specialists could gradually become involved in criminal activities. Next to work relationships, forums also play an important role in criminal collaboration. Forums are used because of a large number of potential partners being available and the appearance of anonymity.

Furthermore, it is worth noting that three out of six analyzed first encounters are immediately directed at criminal collaboration. This could be explained by the existence of equipment that can be used for illegal purposes as well as the feeling of anonymity people experience online. However, as this is a first exploratory analysis, this should be conceived as a hypothesis which requires further empirical testing.

Regarding the level of ICT-expertise, interesting findings are worth summarizing. Even though in four out of five studied cases, advanced technics have been used, most of the persons using these technologies did not have advanced technical skills. This can be explained by the transfer of knowledge on forums and the existence of crimeware-as-a-service. These findings are in accordance with the previous literature on this subject (Leukfeldt et al. 2017a, b, c; Sood and Enbody 2013). Furthermore, it is striking that also employees in the ICT-sector were approached for criminal purposes. Work relationships are easily established because needed goods are legal on the one hand, and there is a gray area on the other hand between legal and illegal services.

These empirical findings regarding criminals seeking ICT-expertise falsify the clear division suggested by Choo (2008). The activities of groups resembling cybercriminal groups contain many elements of traditional crime. It is important to note that money mules were also used in the cases in which the activities mostly took place online. This online-offline connection provides opportunities for combatting this type of crime. This is also true for the online drug markets, as we observed that meetings took place in the physical world and drugs also had to be transported between wholesalers, sellers, and buyers.

Finally, no clear division between traditional offender groups and cybercrime groups has been found, because they both have financial motives and traditional offender groups are, similar to cybercriminal groups, often organized as a network. It is worth noting that both crime groups are more dynamic than is suggested by the term ‘group’. Moreover, it should be mentioned that traditional offender groups are by nature searching for new opportunities and new and old types of crime can intermingle easily. A further intertwinement could be expected in the future. Therefore, future cybercrime research should elaborate upon the intertwinement of both types of crime. Instead of focusing on the differences between cybercriminal groups and traditional groups, future research should focus on the broad spectrum of crimes in which ICT plays a role. Future studies could provide more insight into the implications of innovations for both criminal networks and criminal investigation.

Although these exploratory analyses of criminal investigations provide unique insight into criminals seeking ICT-expertise, they also have some limitations (see Kleemans 2014). Since this study is based on criminal investigations and interviews with police officers, only knowledge is gained about criminals known to the police. As a consequence, no knowledge is gained about criminals that operated very successfully, and thus remained undetected. Furthermore, it should be taken into account that the focus of the police determines the cases that are investigated. This is why many illegal online markets and banking fraud cases came forward in the inventory, and other cases were harder to come across. Follow-up research into criminals seeking ICT-expertise is needed to complement the findings of this exploratory research. This could be done by carrying out interviews with ICT-specialists and studying more conversations on forums. Because this study was conducted solely in the Netherlands, further research should also be done in other countries. This way, it can be explored if such studies would paint a different picture due to differences in policing priorities and information.

This study shows that criminals seek ICT-expertise mostly through work relationships and forums. Moreover, half of the first encounters are immediately directed at criminal collaboration. On the basis of these findings, one could discuss ways in which to increase the perceived exertion, to increase the perceived risk, to decrease the perceived profits, and to take away excuses (Clarke 1997). In the selected cases, trust does not seem to play an important role, giving rise to collaborations in which the initial contact is immediately directed at criminal collaboration. This is why it is important to focus on ways in which feelings of anonymity on forums can be decreased. Furthermore, police investigations could operate actively on forums in order to increase the perceived risk of detection and conviction. Finally, police investigations could be directed at companies providing technical and practical support to criminals. The fact that the equipment is often legal, yet most of the clients are criminal, could be the start of a discussion on how to hold these companies accountable for what they sell to which persons for which purposes.

Appendix 1

List of topics

1. General information

   - Total number of suspects
   - Structure of the group
   - Continuity of activities within offender group
   - Names, dates of birth, and other characteristics of main suspects
   - Qualities of the group members

2. Main suspects

   - Profession
   - Criminal record
   - Particulars (work history, specialization, language, etc.)
   - Role within offender group
   - Motives

- (Technical) level of expertise
- Benefits of cooperation
- Costs and risks of cooperation

3. First encounter

- Who takes the initiative?
- Mechanism to get involved (existing social contacts, work, sidelines and leisure activities, negative life events, deliberate recruitment, etc.)
- How and when did cooperation start?

4. Advantages and disadvantages traditional offender group

- Benefits of cooperation
- Costs and risks of cooperation

5. Advantages and disadvantages ICT-specialists

- Benefits of cooperation
- Costs and risks of cooperation

6. Evaluation

- New insights
- Possibilities to falsify previous findings of research?
- Possibilities to verify previous findings of research?
- Possibilities to specify previous findings of research?

7. Implications for policy

- Why were criminal activities easy to carry out?
- Why were criminal activities difficult to carry out?
- Possibilities to increase the perceived exertion
- Possibilities to increase the perceived risk
- Possibilities to decrease the perceived profits
- Possibilities to remove excuses

References

Ablon, L., Libicki, M. C., & Golay, A. A. (2014). *Markets for Cybercrime Tools and Stolen Data. Hackers' bazaar*. Santa Monica, CA: RAND Corporation.

Bernaards, F., Monsma, E., & Zinn, P. (2012). High tech crime Criminaliteitsbeeldanalyse 2012 high tech crime. In *Crime threat analysis*. Driebergen: KLPD, DNRI.

Brenner, S. W. (2001). Is there such a thing as 'Virtual Crime'? *California Criminal Law Review, 4*(1), 1–72.

Bruinsma, G., & Bernasco, W. (2002). Dadergroepen en transnationale illegale markten. *Tijdschrift voor Criminologie, 44*(2), 128–140.

Choo, K. K. R. (2008). Organised crime groups in cyberspace: A typology. *Trends in Organized Crime, 11*(3), 270–295.
Clarke, R. V. (1997). *Situational Crime Prevention: Successful Case Studies*. New York: Criminal Justice Press.
Clarke, R., & Felson, M. (1993). *Routine activity and rational choice*. London: Transaction Press.
Décary-Hetú, D., & Dupont, B. (2012). The social network of hackers. *Global Crime, 13*(3), 160–175.
Dupont, B., Côté, A., Savine, C., & Décary-Hétu, D. (2016). The ecology of trust among hackers. *Global Crime, 17*(2), 129–151.
Europol. (2014). *Internet facilitated organized crime (IOCTA)*. The Hague: European Police Office.
Europol. (2016). *Internet facilitated organized crime (IOCTA)*. The Hague: European Police Office.
Felson, M. (2003). The process of co-offending. In M. J. Smith & D. B. Cornish (Eds.), *Theory for practice in situational crime prevention (volume 16)* (pp. 149–168). Devon: Willan.
Felson, M. (2006). *Crime and nature*. Thousand Oaks: Sage.
George, A. L., & Bennett, A. (2005). *Case studies and theory development in the social sciences*. London: MIT Press.
Glaser, B. G., & Strauss, A. L. (1967). *The discovery of grounded theory: Strategies for qualitative research*. Chicago: Aldine.
Granovetter, M. S. (1973). The strength of weak ties. *American Journal of Sociology, 78*(6), 1360–1380.
Holt, T. J. (2007). Subcultural evolution? Examining the influence of on- and off-line experiences on deviant subcultures. *Deviant Behavior, 28*(2), 171–198.
Holt, T. J., & Bossler, A. M. (2014). An assessment of the current state of cybercrime scholarship. *Deviant Behavior, 35*(1), 20–40.
Holt, T. J., & Lampke, E. (2009). Exploring stolen data markets online: Products and market forces. *Criminal Justice Studies, 23*(1), 33–50.
Holt, T. J., Bossler, A. M., & May, D. C. (2012). Low self-control, deviant peer associations, and juvenile cyberdeviance. *American Journal of Criminal Justice, 37*(3), 378–395.
Holt, T. J., Smirnova, O., Chua, Y. T., & Copes, H. (2015). Examining the risk reduction strategies of actors in online criminal markets. *Global Crime, 16*(2), 81–103.
Hutchings, A. (2014). Crime from the keyboard: organised cybercrime, co-offending, initiation and knowledge transmission. *Crime, Law and Social Change 62*(1), 1–20.
Hutchings, A., & Holt, T. J. (2015). A crime script analysis of the online stolen data market. *British Journal of Criminology, 55*(3), 596–614.
Kenney, M. (2007). *From Pablo to Osama: Trafficking and terrorist networks, government bureaucracies, and competitive adaptation*. University Park: Penn State Press.
Kleemans, E. R. (2014). Organized crime research: Challenging assumptions and informing policy. In J. Knutsson & E. Cockbain (Eds.), *Applied police research: Challenges and opportunities*, *Crime science series* (pp. 57–67). Cullompton: Willan.
Kleemans, E. R., & De Poot, C. J. (2008). Criminal careers in organized crime and social opportunity structure. *European Journal of Criminology, 5*(1), 69–98.
Kleemans, E. R., & Van de Bunt, H. G. (1999). The social embeddedness of organized crime. *Transnational Organized Crime, 5*(2), 19–36.
Kruisbergen, E. W., Van de Bunt, H. G., & Kleemans, E. R. (2012). *Georganiseerde criminaliteit in Nederland. Vierde rapportage op basis van de monitor Georganiseerde Criminaliteit [organized crime in the Netherlands. Fourth report of the organized crime monitor]*. Den Haag: Boom Lemma.
Lavorgna, A. (2015a). Organised crime goes online: realities and challenges. *Journal of Money Laundering Control, 18*(2), 153–168.
Lavorgna, A. (2015b). The online trade in counterfeit pharmaceuticals: New criminal opportunities, trends and challenges. *European Journal of Criminology, 12*(2), 226–241.
Lavorgna, A., & Sergi, A. (2014). Types of organized crime in Italy. The multifaceted spectrum of Italian criminal associations and their different attitudes in the financial crisis and in the use of internet technologies. *International Journal of Law, Crime and Justice, 42*(1), 16–32.
Leukfeldt, E. R. (2014). Cybercrime and social ties. Phishing in Amsterdam. *Trends in Organized Crime, 17*(4), 231–249.
Leukfeldt, E. R., Kleemans, E. R., & Stol, W. P. (2017a). Cybercriminal networks, social ties and online forums. Social ties versus digital ties within phishing and malware networks. *British Journal of Criminology, 57*(3), 704–722.
Leukfeldt, E. R., Kleemans, E. R., & Stol, W. P. (2017b). A typology of cybercriminal networks: From low-tech all-rounders to high-tech specialists. *Crime, Law and Social Change, 67*(1), 21–37.
Leukfeldt, E. R., Kleemans, E. R., & Stol, W. P. (2017c). Origin, growth and criminal capabilities of cybercriminal networks. An international empirical analysis. *Crime, Law and Social Change, 67*(1), 39–53.

Longe, O., Ngwa, O., Wada, F., Mbarika, V., & Kvasny, L. (2009). Criminal uses of information & communication technologies in sub-Saharan Africa: Trends, concerns and perspectives. *Journal of Information Technology Impact, 9*(3), 155–172.

Lu, Y., Luo, X., Polgar, M., & Cao, Y. (2010). Social network analysis of a criminal hacker community. *Journal of Computer Information Systems, 51*(2), 31–41.

Lusthaus, J. (2012). Trust in the world of cybercrime. *Global Crime, 13*(2), 71–94.

Martin, J. (2014). Lost on the silk road: Online drug distribution and the 'cryptomarket'. *Criminology and Criminal Justice, 14*(3), 351–367.

McGuire, M., & Dowling, S. (2013). Chapter 1: Cyber-dependent crimes. *Cyber crime: A review of the evidence* (Home Office Research Report 75 ed., pp. 4-34).

Odinot, G., Verhoeven, M. A., Pool, R. L. D., & De Poot, C. J. (2016). *Cybercrime, organised crime and organised cybercrime in the Netherlands: Empirical findings and implications for law enforcement*. The Hague: WODC.

Reuter, P. (1983). *Disorganized crime: The economics of the visible hand*. Cambridge, MA: MIT Press.

Sood, A., & Enbody, R. (2013). Crime-ware-as-a-service: A survey of commoditized crimeware in the underground market. *International Journal of Critical Infrastructure Protection, 6*(1), 23–38.

Soudijn, M., & Monsma, E. (2012). Virtuele ontmoetingsruimtes voor cybercriminelen. *Tijdschrift voor Criminologie, 54*(4), 349–360.

Soudijn, M. R. J., & Zegers, B. C. H. T. (2012). Cybercrime and virtual offender convergence settings. *Trends in Organized Crime, 15*(2), 111–129.

van de Bunt, H. G., & Kleemans, E. R. (2007). *Georganiseerde criminaliteit in Nederland: Derde rapportage op basis van de Monitor Georganiseerde Criminaliteit* organized crime in the Netherlands. In *Third report based on the organized crime monitor*. Den Haag: WODC.

Wall, D. (2007). *Cybercrime: The transformation of crime in the information age*. Cambridge: Polity.

Williams, P. (2001). Organized crime and cybercrime: Synergies, trends, and responses. *Global Issues, 6*(2), 22–26.

Yip, M., Shadbolt, N., & Webber, C. (2012). *Structural analysis of online criminal social networks*. 11-14 June 2012. Washington: ISI.

Yip, M., Webber, C., & Shadbolt, N. (2013). Trust among cybercriminals? Carding forums, uncertainty and implications for policing. *Policing & Society, 23*(4), 516–539.

Zabyelina, Y. G. (2017). Can criminals create opportunities for crime? Malvertising and illegal online medicine trade. *Global Crime, 18*(1), 31–48.

Zittrain, J. L. (2006). The generative internet. *Harvard Law Review, 119*(7), 1974–2040.