Wetenschappelijk Onderzoek- en Documentatiecentrum
Ministerie van Veiligheid en Justitie

Cahier 2017-1

Organised Cybercrime in the Netherlands

Empirical findings and implications for law enforcement

G. Odinot
M.A. Verhoeven
R.L.D. Pool
C.J. de Poot

Cahier
De reeks Cahier omvat de rapporten van onderzoek dat door en in opdracht van het WODC is verricht.
Opname in de reeks betekent niet dat de inhoud van de rapporten het standpunt van de Minister van Veiligheid en Justitie weergeeft.

This project has been funded with support from the European Commission with co-financing from the WODC (HOME/2012/ISEC/AG/4000004382); EU Project Cyber-OC - Scope and manifestations in selected EU member states.

Acknowledgements

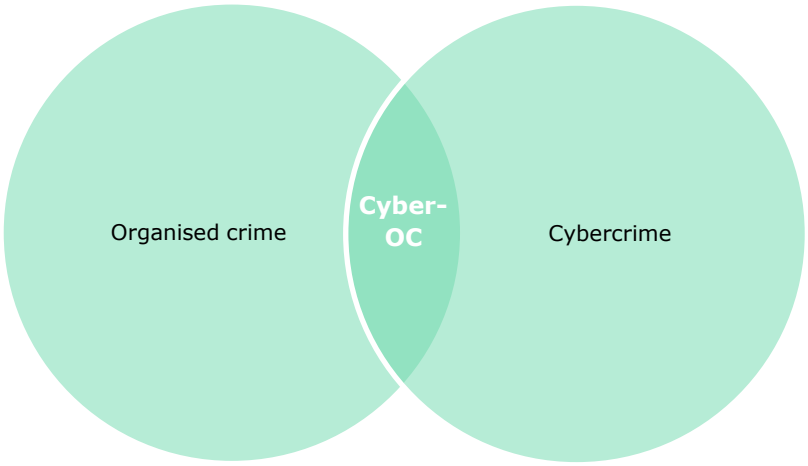
During this project, the researchers had the assistance and input of several people. We would like to thank Ruud Kouwenberg, Renushka Madarie and Mark Engelhart for their work on the data collection. We also had the input of several experts on the topic of cybercrime. We would like to thank them for giving us feedback and their patience in explaining complex technical topics.

Content

Summary

Aims of the study

The growth of cybercrime and increased vulnerability to become the victim of a cyber offence concern the public, law enforcement and policy makers. However, not much information is available yet about the nature and organization of those crimes. Our research explored how criminal groups involved in criminal activities on, via and against the Internet operate by focusing on their modus operandi, the organisational structures of the crime groups, and the profiles of the offenders involved in these groups. We also addressed the ways in which law enforcement agencies investigate these forms of cybercrime and the challenges and obstacles they encounter. By 'cyber organised crime', or 'Cyber-OC' (see also Bulanova-Hristova et al., 2016) we mean the overlap between organised crime and cybercrime, in other words the links and convergence between cybercrime and organised crime.



Other aims of the study are to explore: if the Internet provides new windows of opportunity for illegal business ideas and for the identification and approaching of new targets?; and if the Internet lead to structural changes in organised crime?

Methods: police files and interviews

To find answers to our research questions, different research methods were used. An analysis is made of the police files of criminal investigations into cyber organised crime. We selected eleven cases in which the police inquiries have been completed. The suspects in our selected cases were active in a number of different forms of cybercrime: distributing malware, hacking, running botnets, phishing, abusing the banking system, (digital) money laundering and illegal online trading. Most of the cases have already been tried and judged (ten), and one is still before the courts. The cases were initiated between 2009 and 2014. The eleven files examined, describe a total of 107 suspects.
Next to the police files, we interviewed twelve law enforcement officials to gather information. These officials are working as public prosecutors, police officers of investigating teams, and representatives of the Electronic Crimes Task Force and

Europol. The data for this study was originally gathered in the context of an international research project funded by the European Commission (see also Bulanova-Hristova et al., 2016).[1]

Results: traditional groups and new alliances

Among the case files analysed, we saw on the one hand, traditional crime groups engaging in cybercrime to perform their (traditional) criminal activities more efficiently or in a more sophisticated way. For example, selling drugs online, or using the Internet and encryption in their 'internal' communication. On the other hand, there are new groups developing specific cyber-related criminal activities, new crimes in fact (DDos attacks, distributing malware and ransomware). The new emerging issues and challenges related to cyber-OC we encountered in this study mainly originate from these new online activities.

New opportunities: new ideas, new targets

Next to anonymity, crime as a service and the option to use fora, this study has shown that the Internet provides for new business ideas and new targets. In this way ICT functions as a tool to increase the efficiency and economic gain of crimes. Considering the new marketing channels, this has lead to new opportunities to get in touch with targets. In the end, one could also argue that through new opportunities caused by globalisation these 'new' crimes are rather an evolution of traditional crimes.
This development makes crimes that require coordinated activities seem less complex and more accessible to larger groups of people. This leads, apart from changes in the modus operandi and changes in the target groups, to (1) new players in the field, (2) new forms of collaboration and (3) new economic structures.

1 New Facilitators

Most notable are new facilitators, consisting on the one hand of people who are technically skilled, and on the other hand of (legitimate) companies (private parties), such as hosting providers, online advertising firms, web shops, courier firms (postal companies) and telecommunication companies. We also encountered new kinds of front businesses, bitcoins exchangers and money mules who facilitate illegal activities. These facilitators in the digital world are not the same parties as we know from offline organized crime cases and offer new possibilities for law enforcement and prevention in the field of cybercrime. It could be worth to invest in prevention, detection and involvement of these parties, for example in public-private co-operations.

2 Collaboration and organisation

The ways suspects cooperate are partly comparable to other forms of organised crime. Similarities are:

- *Dynamic networks*: criminal alliances are changeable; people get involved and people drop out.
- *Based on social relationships*: in our cases family ties, friendships and exclusively online relationships all appear within collaborations.

[1] EU Project: Bulanova-Hristova et al. (Eds.) (2016). Cyber-OC - Scope and manifestations in selected EU member states (HOME/2012/ISEC/AG/4000004382).

There are also aspects of organised cybercrime that differ somewhat from other forms of organised crime:

- *Anonymity in cyberspace*: online activities can be conducted anonymously, and offline contact between 'partners in crime' is not necessary to commit online (criminal) activities. This makes cooperation less risky and changes the role of trust within criminal cooperation.
- *Crime as a service*: certain tasks can be bought online as services, which gives the organisation of cybercrime a new or different dimension. ICT-skilled people can sell their services to other online or offline active suspects. Within this 'cooperation', different individuals undertake specific activities and there is no real need for them to make contact before the task is complete.
- *Role of forums*: online cybercrime forums seem to provide a meeting place for criminals and function as communication channels. They facilitate the collaboration between suspects and lead to the formation of new collaborations between suspects active on these forums. Through this way suspects are able to build online relationships and collaborate and communicate without meeting each other offline. The channels are used for selling and sharing knowledge, software, scripts, goods, products and raw materials. The fact that online communication services mostly use encryption appears to be an important motivation to use these forums instead of more traditional communication channels.

Chain-structures and divided responsibilities

As a result of these opportunities, in contrast to more traditional organized crime groups, the newer groups emerging in the cyber field, sometimes seem to differ in their approach to a *long-term perspective* on their co-operation. Although individuals seem to have a long-term perspective regarding their own activities, the alliances involved in a particular crime are often less stable and do not always share a long-term perspective on conducting ongoing criminal activities within the same alliances. It seems to be less necessary to form a stable group, since the quality of one's contribution seems to be more important than trust between co-operating people. Due to the anonymity of online collaborations, this collaboration is less risky, and building trust is less important in these cyber-OC groups. Within these more loose networks or alliances the cooperation between suspects can take the form of a chain, linking people involved in different activities, which together constitute a criminal act. In these chain-like collaborations, suspects work together, but are responsible for only a single part of a crime. As a consequence, suspects can get involved in organised crime without knowing exactly what they are involved in. Within these chain-like structures, in a way, every suspect has power, and every suspect has a certain role, but either everyone or no one seems to be responsible for the crime as a whole. There might not even be an intended goal. This appears to be quite a new characteristic of organised crime, manifesting itself in cyber-OC cases that we did not see before and that definitely changes our concept of what organised crime entails. In such a chain structure, the different players can all act for themselves and achieve private goals. Together they accomplish an organised form of crime, using the bottom-up approach rather than being organised top-down. This way, crimes as well as crime groups seem to more or less co-incidentally arise and take on a certain form.

Because of these developments, cyber-OC can be committed either under mutual arrangements between offenders (suspects knowing each other and working together on a criminal project, relying on the division of tasks) or without any coordination in a chain environment. As a result, there is huge diversity and uncertainty, and it

may become difficult to allocate crimes to specific crime groups or criminal organisations and to predict how crimes will take shape.

3 New economic structures
New economic structures relate to the use of cryptocurrencies to transfer and launder money via the Internet. This has created new underground economic structures that are difficult to control. It would be interesting to examine to what extent rules, reporting systems and inspection bodies in the field of unusual transactions could also apply and be used for cryptocurrencies.

Criminal investigation of organised cybercrime

Anonymity online and the identification of suspects
The special cybercrime team of the Dutch Police – the National High Tech Crime Unit – has grown rapidly during the last years. This means capacity and expertise is reserved for the criminal investigation of cybercrime cases. However, the amount of possible cybercrime cases rises and the police is forced to fix priorities in detecting and investigating cases.

Special investigative powers
The wide array of sophisticated technical methods to act anonymously on the Internet, require the use of special investigative powers to reveal people's identity. These investigative powers can be applied both online and offline. The upcoming new Computer Crime Bill offers the police new investigative tools, and creates possibilities to get access to information before it is encrypted.

Information position on the Internet
To get grip on traditional organized crime groups, the Dutch police has a special unit, the Criminal Intelligence Unit (CIU). People from the CIU can work undercover with some people in a criminal group and provide information about criminal activities. This information is often used as a starting point for a criminal investigation. However, according to our interviewees, the information position within the Internet community needs attention. Several of our interviewees think that developing this in the future, would be valuable in the fight against cybercrime.

International cooperation
Since a suspect on the Internet can physically be anywhere; identifying, localising, arresting and finally convicting suspects often requires thorough international collaboration. Our interviewees are positive about the facilitating role of Europol within international cooperation. However, the success of Joint Investigation Teams appear to be heavily dependent on capacity and priorities in the collaborating countries. In police investigations that do not have the formal status of a JIT, formal requests to other jurisdictions are required for assistance or information. Due to different priorities, complicated paperwork or political difficulties, these requests are often dealt with a pace that is incompatible with the speed of the Internet. Overcoming these kinds of problems would be a real gain in investigating (organised) cybercrime.

1 Introduction and methods

1.1 Purpose of the study

Over the years, our lives have become increasingly digitalised and intertwined with computers and the Internet. Being connected to the Internet, where we store personal data in the cloud, pay bills, order food, and communicate, is daily routine for many people. This digitalisation of society is proceeding rapidly worldwide. More digital applications, devices and tools make it possible to share and store information when connected to the Internet. This does not only hold for individuals; commercial companies, non-profit organisations, banks, hospitals, and governments also digitalise and store their information on devices that are often part of the Internet or linked to the Internet. These developments however, also come with new opportunities to commit crimes. For instance, digital services or websites can be shut down by hackers, data can be stolen, changed or destroyed, bank transactions can be interfered with by cybercriminals, personal computers can be blocked at a large scale, money can be laundered online and drug smugglers can use the Internet to buy or sell substances. It is clear that organised crime groups have found their way to computers and the Internet to commit serious crimes. Over the years, committing cybercrime has become easier. It requires less technical expertise, because modus operandi are shared online and can be bought from others (Richet, 2013). McAfee describes cybercrime as a 'growth industry', were the profits are large while the risks are low.[2] According to news websites, this type of crime costs the Dutch economy some 8.8 billion euros annually, or approximately 1.5%of the gross national product (McAfee Center for Strategic and International Studies, 2014, p. 9). For law enforcement it is challenging to keep up with this type of crime because technological developments go fast and the digital environment is often complex. To investigate and prosecute cybercrime, law enforcement agencies require capacity as well as skilled investigators and prosecutors.

The growth of cybercrime and the increased risk to become the victim of a cyber offence concern the public, law enforcement agencies and policy makers. In this study we aim to shed light on a specific aspect of cybercrime, namely the linkage between cybercrime and organised crime. To what extent is cybercrime organised? To what extent are existing organised crime networks involved in cybercrime? And how do our law enforcement agencies deal with 'cyber organised crime'? The term Cyber Organised Crime (cyber-OC) is used to denote cases involving both cybercrime and organised crime. Knowledge and understanding of the nature of cyber organised crime and of the problems law enforcement agencies encounter when investigating these crimes can help to develop and improve strategies to counteract these crimes.

The Internet operates without geographical borders and offers people the opportunity to hide their identity and the location from which they operate. This allows offenders of cybercrime to remain anonymous, which brings about new challenges for law enforcement agencies. Europol states that due to the difficulty to identify offenders as well as the problems that arise when identified offenders reside in countries that have no extradition treaty with the European Union, it is extremely difficult to investigate and prosecute cybercrime.[3] Organised crime has always been

[2] www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf

[3] Infosecurity Magazine, 30 april 2014 'Europol wil cybercriminelen actief gaan hinderen, see: http://infosecuritymagazine.nl/2014/04/30/europol-wil-cybercriminelen-actief-gaan-hinderen/

difficult to investigate and to prosecute (Van de Bunt & Kleemans, 2007; Bokhorst, Van der Steeg & De Poot, 2011; Verhoeven, Van Gestel & De Jong, 2011; Van Wingerde & Van de Bunt, 2016). In case of cyber-OC, where organised crime and cybercrime are intertwined, these crimes will be even harder to comprehend and to fight. Therefore it is important to analyse how different forms of cyber-OC manifests themselves in the Netherlands, and what law enforcement agencies can do to counter these crimes.

A recent review of the literature on the links between organised crime and cybercrime (Dietrich, Kasper & Bulanova-Hristova, 2016) shows that empirical research on cyber-OC is still in its infancy. Hence, many questions regarding the manifestations of these crimes cannot be answered satisfactorily. How do Dutch law enforcement agencies deal with cyber-OC? What investigative means or strategies are used? Do investigations into cyber-OC result in the detection of offences and offenders? And if so, what do these investigations reveal on this phenomenon?

This study aims to provide insight into the links between organised crime and cybercrime in the Netherlands, and to indicate the significance of these findings for law enforcement agencies. By exploring the specific characteristics of the offenders, organisational structures and crime activities on, via and against the Internet we hope to provide insights that can be used to develop ways to prevent, investigate and counter cyber-OC.

The data for this study were gathered in the context of a research project funded by the European Commission.[4] In this project we cooperated with researchers from Germany[5] and Sweden[6], who also answered the abovementioned research questions for their countries.[7]

1.2 Cybercrime and organised crime

The fight against cybercrime is a top priority on the political agenda of the EU and of individual member states for quite some time. During the past years, the Research Centre of the Dutch Ministry of Security and Justice (WODC) has conducted a significant number of studies on different aspects of cybercrime for the purpose of security and justice policy in this area.

Examples are research projects into the nature of cybercrime, which consist of general literature overviews and reviews (Scheepmaker, 2004, 2012; Van der Hulst & Neve, 2008), studies on more specific crime acts, like online money laundering (Oerlemans, Custers, Pool & Cornelisse, 2016), Internet-facilitated drug trade (Kruithof, Aldridge, Décary-Hétu, Sim, Dujso, Hoorens, 2016), and the involvement of youth in cybercrime (Zebel, De Vries, Giebels, Kuttschreuter & Stol, 2013; Van den Broek, Weijters & Van der Laan, 2014). This subject is also addressed in the on-going monitor juvenile crime (Van der Laan & Goudriaan, 2016). In addition there is methodological research on measuring cybercrime (De Cuyper & Weijters, 2016); research on the international policy on cybersecurity (Adams, 2015), and there are several studies on legal aspects of tackling and investigating cybercrime (Koops, 2012; Koops, Leenes, De Hert & Olislaegers, 2012; Koops & Goodwin, 2014); Finally there are studies on the shortage of cyber security professionals

---

4 EU Project Cyber-OC - Scope and manifestations in selected EU member states (HOME/2012/ISEC/AG/4000004382).

5 Researchers from the German Federal Criminal Investigation Department – Bundeskriminalamt (BKA).

6 Researchers from the Swedish National Council for Crime Prevention – Brottsförebyggande rådet (Brå).

7 See Bulanova-Hristova et. al. (2016) for the full report on this study, in which research findings from all three countries are integrated.

(Lakerveld et al., 2014) and on the investments and initiatives of organisations in cybersecurity (Van der Meulen, 2015; Hulsebosch & Van Velzen, 2015).
Next to WODC-studies, the studies of Rutger Leukfeldt are relevant in this context. He conducted several studies on the origin, growth, structure and modus operandi of cybercriminal networks (and on the differences with traditional criminal networks) (Leukfeldt, 2014; Leukfeldt, 2015; Leukfeldt, 2016). His data concerned cybercrime that targeted the customers of financial institutions. He found that despite the options that digitization provides, real-world social ties are important for the majority of these cybercriminal networks for their origin and growth (Leukfeldt, 2014; Leukfeldt, Kleemans & Stol, 2016; Leukfeldt, 2016).
In the literature, a variety of different and partly opposed points of view on the organisational structure of cybercriminals can be found (Dietrich, Kasper & Bulanova-Hristova, 2016). Whereas some authors suggest that cybercriminals rather operate alone than in groups, others state that there exist long-lasting, job-sharing organised crime groups in cyberspace, too. Dietrich et al. (2016) found that research regarding cybercrime and organised crime confirms that the latest technical developments are followed and used to commit crimes. In addition to the technical development, the increasing global interconnectedness of people offers new possibilities for committing crimes. Hence, people who commit conventional crimes in the physical environment by means of ICT, but also criminals who exclusively operate in the virtual environment, can profit from amongst others the improved cost and time efficiency as well as from the lower detection risk (ibid).

Since several questions regarding the linkage between organised crime and cybercrime are not addressed yet, this study will focus on the overlap between organised crime and cybercrime. We use the term cyber organised crime or cyber-OC to refer to this overlap (see also Bulanova-Hristova et al., 2016).

1.3 Research questions, method and data collection

This study seeks to explore the characteristics of cyber-OC, and focuses on the criminal activities of cyber-OC groups, their modus operandi, the organisational structures, the 'profiles' of the involved offenders, and the characteristics of criminal investigation into these cases. For this purpose we will focus on the following research questions:

1 Is organised crime involved in cybercrime? What kind of cybercrime do organised crime groups commit?
2 How do organised crime groups use the Internet to commit 'traditional crimes'?
3 Does the Internet provide windows of opportunity for the development of new business ideas and for the identification and approaching of new targets?
4 Does the Internet lead to structural changes in organised crime?
5 Is cybercrime organised? How, why and when?
6 How does the criminal investigation of (organised) cybercrime work in practice and which best practices and challenges can be identified?

To answer these questions, different research methods were used. Next to an analysis of police files, interviews were held with experts from law enforcement. Below, we will describe our methods in more detail.

1.3.1 Police files

We tried to select cases that provide insight into cyber-OC. The selection of cases was made together with law enforcement experts who knew all the cases that met the predefined criteria and could indicate which cases would be the most interesting given our research questions. With the criteria we aimed to select closed criminal investigations which handled about the overlap between cybercrime and organised crime. Next to this we pursued that a variation of criminal activities was represented in our selection.
From a list of all organised cybercrime inquiries, experts from the police and the public prosecution pointed out the most interesting cases for our study. Because we wanted to gather data about as many aspects of the phenomenon as possible, we asked them to choose cases offering the greatest value from that perspective. We did not confine ourselves to any particular type of crime or modus operandi, but instead sought a wide variety of offences that could be described as cyber-OC in the broad sense and the narrow sense of the term. We did not set any requirements as to the proportion of cases falling into each of these two categories, since that might have hindered the search for interesting files. However, we were particularly interested in inquiries with an international dimension.
We also expressed a clear preference for recent case files, given that technological developments and innovations are constantly changing the way cybercrime manifests itself. The pool of cases that met our criteria turned out to be rather small. With help from the experts we were able to select eleven cases in which the police inquiries had been completed. These eleven cases constituted about half of the available cases. According to the experts, these cases collectively provide a good reflection of the phenomenon, and of the investigations into this phenomenon. Two of the cases were initiated in 2009, one in 2010, three in 2012, four in 2013 and one in 2014. In the eleven selected files, a total number of 107 identified suspects were active. At this moment (January 2017) all but one have been tried and judged. We deliberately chose to analyse cases that provide insight into various forms of cyber-OC encountered in the Netherlands, rather than studying all available cases. In order to gain access to the relevant files, we contacted the National Cybercrime Prosecutor and the National High Tech Crime Unit (NHTCU) of the National Police, who made the cases available for study and analysis.

Studying police files is valuable, because they contain information on the alleged facts, the suspects, the victims, witness statements, transcripts of police interrogations, as well as information on the police investigation itself. By using extensive investigative methods, such as infiltration, wiretapping, recording of confidential communications and observation, these investigations provide unique knowledge about the behaviour of offenders and the way they collaborate (Van de Bunt & Kleemans, 2007).

Checklist
Of each selected case, we analysed the police files, using a checklist to select relevant information from the files. This checklist was used as an analytical tool in order to keep the same focus and extract the same type of information from all the files.
The checklist, was an adapted version of the method that was originally developed by Kleemans et al. at the end of the nineties to investigate the nature of and developments in organised crime in the Netherlands (see Kleemans, Van den Berg & Van de Bunt, 1998; Kleemans, Brienen & Van de Bunt, 2002; Van de Bunt & Kleemans, 2007; Kruisbergen, Van de Bunt & Kleemans, 2012). Specific topics that are rele-

vant to cybercrime were added to the original checklist. For instance, a question about how people were gaining trust of others in online relations, and a question about currency used to launder money or to pay for goods. Using the checklist resulted in a large pool of qualitative data extracted from the selected police files. To analyse this dataset further, we coded the data in the checklists with the use of MaxQDa, a software tool for the analysis of qualitative data.

1.3.2 Interviews with experts

Next to analysing the police files we interviewed 12 law enforcement officials to gather information about cyber-OC. In order to study each of the selected inquiries and to obtain background information, we contacted the public prosecutors or the police investigators who had been in charge of the investigation. These key players were interviewed about one or more of the cases they worked on. In some instances, this was done after the file had been examined. In those cases the interviews were focused on finding answers for remaining questions. In more complex cases, however, a semi-structured interview was conducted with either the leading public prosecutor or (in one instance) the secretary at the public prosecutor service overseeing the full inquiry, before we looked at the files in any detail. This was done in order to get an impression of the characteristics of the case. Particularly in case of large and wide-ranging investigations that have produced large case files, this approach was necessary to understand the essence of the case from the outset, as well as how the material was structured and what issues it raises. But here, too, we retained the option of asking additional questions to persons directly involved in the investigation at a later stage, after the file had been studied at greater length.
We also wanted to learn more about the roles played by the Electronic Crimes Task Force (ECTF)[8] and Europol in tackling organised cybercrime in the Netherlands, so representatives of these organisations were contacted as well.

1.4 Limitations

The research methods we used have some significant limitations. On the basis of the analysed investigations we can describe the characteristics of cyber-OC networks that were active in the Netherlands between 2009 and 2014; the activities that were performed within these networks, and the suspects involved, insofar as this is revealed by the selected criminal investigations. Firstly, the selection of available criminal cases the police investigated may have influenced our perception of the phenomenon. Secondly, police files provide a lot of information about offenders, activities and criminal collaborations, as well as on police tactics and investigative tools. However, we may not assume that the police files give a complete picture of all the social ties that exist in a criminal network, and of all the criminal activities conducted within this network. For instance, communication between suspects can be encrypted and often it is difficult to identify people on the Internet. Without any doubt, there is information which is not traced by the police and which is thus unavailable for this study. Besides, when there is enough evidence gathered to bring a case to court, the public prosecutor mostly decides to stop the investiga-

8 A partnership between banks, the police force and the Public Prosecution Service. This partnership was established to strengthen the information position of all parties and to improve the quality of detection, prosecution and intervention.

tion. The information in Dutch police files is therefore not exhaustive and complete. This should be kept in mind when interpreting our research results.

1.5 Structure of the report

In chapter 2 we outline the Dutch criminal justice system, its procedures, and the relevant laws and institutions concerning the way cybercrime is addressed in the Netherlands. In chapter 3 empirical findings are presented on the suspects, the way in which they collaborate, the activities they conduct and their modus operandi. Chapter 4 deals with criminal investigation processes into cyber-OC. In chapter 5 we draw conclusions.

2 Organisation of investigation and prosecution in the Netherlands

This chapter describes the structure of the Dutch criminal justice system. The roles of the various players in the investigative process and the chain of justice are explained in brief so as to provide the reader with a context for the Dutch cases discussed in this chapter. We also provide a basic introduction to the legislation governing the methods often used in the Netherlands in the investigation of organised (cyber)crime.

In this chapter we use the term cybercrime. This has become a popular term for all forms of Internet-related crime, although official Dutch legal terminology still uses the expression 'computer crime' in reference to any unlawful activity involving computer technology. In this report, however, we use the term 'cybercrime', which is increasingly used internationally, in both the scientific literature and the popular media. In order to tackle this form of crime, Dutch police work closely with public parties such as the National Cybersecurity Centre), private parties and the non-profit sector. Special teams have been established to fight online banking fraud, child pornography and 'high-tech' crime, and because cybercrime is often an international phenomenon the police also conduct investigative work in collaboration with Europol, Interpol and foreign police teams (see Van der Leij, 2014 and Tak, 2008). Below we outline the general organisation of criminal investigation and prosecution in the Netherlands and introduce the actors involved specifically in the investigation of cybercrime.

Identifying those committing cybercrime and bringing them to justice are police tasks, although ultimate responsibility rests with the Public Prosecution Service. Police investigations are conducted under the supervision of public prosecutors, in consultation with the police; it is the former who decide which cases to pursue, what investigative methods to employ and whether to charge and prosecute suspects. The investigations are a task for the police.

The Dutch police is a national force subdivided into ten regional units, a Central Unit and a national Police Services Centre, which comprises the various support departments. It is headed by a commissioner. The ten regional units undertake all operational policing duties, apart from those requiring specialist expertise, which are performed at the national level and so are entrusted to the National Police Agency. Each regional unit is further subdivided into local, district and regional teams, all of which carry out criminal investigation work. Those at the district levels focus on common 'everyday' offences, also tackling crimes with a major impact on victims, such as robberies. In addition, detectives specialising in specific fields, such as digital investigation, juvenile offenders and financial crime, are also active at the district level. At the regional level, there are investigative teams dedicated to criminal organisations and to serious forms of crime such as human trafficking, vice, child pornography, fraud and cybercrime. Requests for assistance from other agencies are also handled at the regional level. The Criminal Investigations Division concentrates mainly upon various forms of organised transnational crime and other serious offences requiring a high degree of specialist investigative expertise. The National High Tech Crime Unit (NHTCU) is also part of this division.

The Public Prosecution Service is similarly divided into ten regions, coinciding with those covered by the regional police units. The service also has a National Office dedicated to the fight against domestic and international organised crime, including organised cybercrime, and a Special Office to deal with environmental, economic and fraud offences.

The prosecution service's governing body is the Council of Attorneys-General. Together with the Minister of Security and Justice, it determines national investigation and prosecution policy. The minister bears political responsibility for both the police and the Public Prosecution Service.
Under Article 10 of the Dutch Code of Criminal Procedure (DCCP, in Dutch: *Wetboek van Strafvordering*), all criminal investigations are formally led by a public prosecutor. The public prosecutor determines how investigative resources are deployed and, based upon the results obtained, decides whether or not to prosecute a suspect. This is known as the discretionary prosecution principle (also called opportunity principle) and allows the Dutch Prosecution Service to decide whether or not to continue with a case.
Before using certain investigative powers, the public prosecutor must first obtain authorisation from an investigative judge – a special judge who oversees the preliminary investigation before it goes to trial. As well as being entitled to examine witnesses and appoint expert investigators, the investigative judge rules on police or Public prosecutor applications to extend periods of detention without charge and for warrants to open mail, intercept telephone calls, search residences and so on. In the case of requests for such special investigative powers, in order to protect the rights of the suspect, the investigative judge considers whether their authorisation is reasonable and proportionate, and subsequently checks that the conditions imposed for their use have been complied with (DCCP).[9]

2.1 Criminal investigation of cybercrime in the Netherlands

Political interest in the fight against cybercrime has increased in recent years. In 2014, McAfee reported that cybercrime is costing the Netherlands at least 8.8 billion euros a year.[10] There are also indications that organised crime is becoming more and more involved in cybercrime (Van der Hulst & Neve 2008, p. 33). Investigating and countering this form of crime requires specialist expertise and methods on the part of the police. In order to respond to developments and provide the necessary expertise, substantially increasing anti-cybercrime capacity, it was decided to establish a special High-Tech Crime Team at the national police squad. This formed in 2007 with a full-time equivalent workforce of 15, which had risen to 120 by the end of 2014 (CotEU 2015, p. 21; Wervingsfolder Politie [Police recruitment brochure] 2013, p. 5.). Its focus is on cybercrime attacks with an impact on national levels that undermine information security, use innovative technologies and cause widespread social harm (so-called 'high-impact' crimes) (CBA 2012, p. 12). Compared with the staff in other police units, a large part of this team has an IT-background instead of a policing background.
Despite its relatively large staff, the NHTCU can only take on a limited number of cases each year. In practice, the team has to prioritise the investigation of certain cases, resulting in a large proportion of cybercrime left untouched. In order to overcome this, it has been decided to extend investigative capacity in this field to the regional police units (Min. VenJ, 2014). In these regional units, cybercrime cases are investigated by general investigation teams, supported by digital experts. In order to provide sufficient digital support these units are forming their own dedicated teams of 'cyber investigators'. This way, the NHTCU can concentrate on

[9] For more information about the assessment criteria for Public prosecutor applications for warrants to intercept communications and their authorisation by an RC, see Hoge Raad (Supreme Court of the Netherlands), 11 October 2005, LJN AT 4351.

[10] www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf.

larger, more complex cases and cases of national importance. As one member of that team put it in an interview, 'Today's high-tech crimes are tomorrow's everyday cybercrimes'. The idea is that the NHTCU itself will handle only innovative, technically complex, nationally important cases, sharing its operational expertise with the regions. And the bulk of cybercrime will be dedicated to the regional police. That is not to say investigations into international cases cannot be conducted at the regional level.
At present, cases are allocated by a survey team consisting of police and public prosecutors, taking availability of time and capacity into account. Just like many larger drug cases, which are also dealt with by regional teams, a lot of cybercrime is not confined to a single locale or jurisdiction.

This does pose a challenge for the future, however. As yet, there is no single central point the regions can call upon for information. Moreover, as capacity is limited, the cyber cases in the regions have to compete with investigations into other serious crimes like murder and drug trafficking. These, too, may have an IT component, which diverts the expertise of 'digital' detectives.
In 2015, the Ministry of Security and Justice allocated an annual budget of 13.8 million euros specifically to improve the police's ability to fight cybercrime at the regional level (CotEU 2015, p. 20). Under the 2014 Tactical Programme for High-Tech Crime, the NHTCU is required to reserve 40%of its investigative capacity to handle requests for assistance from other agencies and for incident-led inquiries. The remaining 60%is devoted to the team's so-called priority areas: cyber attacks on vital infrastructure and the financial system and investigations of ransomware, facilitators and botnets (Landelijk Parket, 2014, p. 20).
This increased focus upon cybercrime is also reflected in the general goals being pursued by the Ministry of Security and Justice. Amongst them, reducing this form of crime and intensifying efforts to bring its perpetrators to justice are listed as priorities (Min. VenJ, 2014, p. 5). Similarly, the police's published policy objectives include both an overall increase in the number of 'regular' cybercrime investigations and expanding the NHTCU's 'complex' caseload. The ministry's Public Security Agenda for 2015–2018 enumerates the annual targets as follows (see table 1; Min. VenJ, 2014, p. 5).

Table 1 Overview cybercrime investigations 2014-2018

Year	2014	2015	2016	2017	2018
Complex cases	20	25	30	40	50
Regular cases	180	175	190	230	310
Total	**200**	**200**	**220**	**270**	**360**

'Complex' cases are those of the kinds mentioned in the NHTCU's list of priority areas. They might include hacking a hospital's IT infrastructure, infecting critical systems with a virus or using botnets for criminal activities. 'Regular' cases can be characterised as 'traditional' forms of crime with an added digital component. Because of the huge increase in offences of this kind, dealing with them will require much more digital expertise in the years to come.

Public Prosecution Service and cybercrime
The Public Prosecution Service has moved forward in this domain in recent years. Every district office now has dedicated cybercrime prosecutors, and there is also a National Cybercrime Prosecutor. According to a 2012 report by legal consultancy Pro Forma and the Centre for Law & IT at the University of Groningen, prosecutors at the district level have had little or no engagement with cybercrime cases. They lack

the expertise in this field and do not prioritise these cases. As one of the respondents told the researchers, 'Blood comes before bytes' (Struiksma, De Vey Mestdagh & Winter, 2012, p. 30). This should change once plans to invest in expertise and capacity at the regional level are set in motion. The Ministry of Security and Justice has allocated substantial additional funding to help the Public Prosecution Service intensify its investigations into cybercrime, starting with 1.5 million euros in 2016 and rising permanently to 2.7 million euros a year from 2017 onwards (OM, 2015, p. 4).

National Cyber Security Strategy

As we become more and more dependent on information technology, the Dutch government is working to ensure a safe, secure and stable cyber domain. Its first National Cybersecurity Strategy (NCSS) was published in 2011. An updated version, NCSS 2: 'From awareness to capability', was released by the Minister of Security and Justice at the end of October 2013. Security and freedom play key roles in the Dutch approach, where it is important not to lose sight of basic rights and social development in seeking to ensure cyber security (NCTV, 2013, p. 17).

> *'Working with international partners, the Netherlands aims to create a secure and open digital domain, in which the opportunities digitisation offers our society are used to the full, threats are countered effectively and fundamental rights and values are protected.'* (NCTV, 2013, p. 7)

This policy vision has been translated into an NCSS Action Programme for 2014-2016, (NCTV, 2013, p. 27 (Appendix 1)) with fighting cybercrime, preventing digital intrusions and counter-espionage as its main priorities. According to NCSS 2, measures the Netherlands intends to take in pursuit of these goals include: (Min. van Veiligheid en Justitie, 2014; CotEU, 2015, p. 13; NCTV, 2013, p. 27 et seq.)

- updating and strengthening both domestic and international legislation (for example, through the third Computer Crimes Bill – see below);
- improving collaboration with Europol by sharing more information;
- strengthening the fight against cybercrime in the financial sector through close co-operation with private sector partners;
- increasing the number of international investigations to 20 in 2014;
- ensuring that law enforcement agencies keep up with the increasing digitisation of crime; and
- strengthening the police intake and registration process for official reports of cybercrimes.

With cybercrime, it is important that the police are sufficiently knowledgeable about the issues involved and are able to act quickly, both domestically and internationally (Bernaards et al., 2012, p. 10). Because of the high level of political interest in this domain, the NHTCU has expanded rapidly in recent years. In March 2006, the police opened an online Cybercrime Reporting Centre, a special website where citizens could report instances of child pornography, sex tourism and terrorist activity. In April 2013, this ceased to be a separate platform and these crimes can now be reported on the main police website. However, there is still a special site to report child abuse materials.

Electronic Crimes Task Force

The ECTF is an example of a public-private partnership between law enforcement agencies and banks, allowing information to be shared quickly.

Cybercriminals regularly target large institutions, like banks, with relatively well-protected IT systems (Bernaards et al., 2012, p. 13). Phishing and malware are amongst the methods used by cybercriminals to mislead a bank's clients, exploiting its name in an effort to obtain login details. As well as causing financial loss, this form of deception can harm the institution's reputation and undermine customer and public confidence in it and the entire banking system. In response, at the instigation of a number of major Dutch banks, the Electronic Crimes Task Force (ECTF) was established in 2011.[11]

The ECTF enables participating organisations to share substantial amounts of information; unusual patterns and anomalous transactions can be detected at an early stage. The National Police Service is also a party to the covenant, making it possible to conduct swift background checks on possible suspects and the victims of suspicious transactions. During the collaborative process, a dossier of the information gathered is compiled for submission to investigators as supporting evidence if and when the matter is formally reported. This file also contains information on the nature of the case, the reasons why it should be investigated, and possible leads for further inquiries. Ultimately, though, it is up to the police whether the matter is taken further.

National Cyber Security Centre
The National Cyber Security Centre (NCSC) was founded in January 2012 with the aim of bringing together private and public-sector partners in the fight against cybercrime. Since its focus lies on sharing current information concerning IT threats and cybersecurity incidents,[12] in this respect, the centre relieves the NHTCU and other agencies of some of the burden. The NHTCU is an investigative unit, whereas the NCSC is an information centre that is able to play a coordinating role in the event of an IT crisis. It also updates the public and SMEs (Small and Medium-sized Enterprises) on safe use of the Internet by providing general information and specific current warnings through the website www.veiliginternetten.nl, thus enhancing wider awareness of cyber security issues.

2.2 Legal framework on cybercrime in the Netherlands

Legislation plays a fundamental role in the investigation and prosecution of cybercrime. The origins of the legislation on computer crime in the Netherlands can be traced back a few decades. Before we go into its evolution since then, it is important to clearly define the terms 'cybercrime', 'data' and 'computerised devices' in the Dutch legal context.

Key definitions
The National Police Service defines 'cybercrime' as 'any form of criminal act in the perpetration of which the use of computerised devices or systems to process and transfer data is a significant factor' (Bernaards et al., 2012, p. 11). Although it may seem very sweeping, such a broad definition has its advantages given the fact that cybercrime as a phenomenon is evolving all the time. Moreover, it uses the technology-neutral terms 'data' and 'computerised devices or systems'. The Dutch Criminal Code (*Wetboek van Strafrecht*, DCC) defines 'data' as 'any representation of facts,

[11] ECTF Covenant: www.rijksoverheid.nl/documenten/convenanten/2011/03/15/convenant-samenwerking-en-informatie-uitwisseling-electronic-crimes-task-force; interview with ECTF.

[12] www.ncsc.nl/organisatie.

concepts or instructions in an agreed-upon form suitable for transfer, interpretation or processing by human beings or by computerised devices and systems' (DCC, Art. 80quinquies), which includes software. A 'computerised device or system' is defined in Article 80sexies of the DCC as 'a single device or group of combined devices that automatically process and transfer data'. This is a broad definition, which covers not only computers but also, for example, telephones.
A distinction that is relevant in this context is the usage of the Internet as the *target* of a crime and as a *tool*. This brings us to the two basic categories of cybercrime, 'narrow' and 'broad', with the former encompassing criminal acts in which computers themselves, and their contents in particular, are the target. In other words, these are offences that cannot be carried out without a computer. Examples include hacking, distributing viruses or Trojans and phishing.
Cybercrime in the broader sense means 'traditional' offences carried out with the aid of computers and the Internet.[13] In these cases computers and the Internet are used as significant tools for crime. This often brings an international dimension to the criminal act. Online fraud, webshop swindles and electronic money laundering are examples of this 'broad' category of cybercrime (Kaspersen, 2004; Bernaards et al., 2012, p. 11).

History of the Dutch cybercrime legislation
Over the years, the Dutch Criminal Code (DCC) and Dutch Code of Criminal Procedure (*Wetboek van Strafvordering*, DCCP) have been updated gradually to include new technology-neutral provisions applicable to cybercrime in all its forms. In 1988, the Computer Crime Commission also known as the Franken Commission, published a report on 'Information Technology and Criminal Law', examining how the existing legislation should be revised. One important aspect of this publication was that the commission drew a clear distinction between 'data' and 'goods'; whereas goods are more or less unique by nature, one of the characteristics of data is that it is universal – more than one person can possess the same data at the same time (Koops, 2007, p. 19; cf. Kaspersen, 1990). Another significant landmark was the report's proposal that 'computer trespass' – hacking – be made a criminal offence. The first Computer Crime Act (CC I) came into force in 1993, largely inspired by the commission's report. As the commission had also pointed out, however, the battle against computer crime cannot be fought through legislation alone. For this reason, the new law's provisions against 'computer trespass' incorporated a security requirement – the user must take reasonable measures to prevent intrusion. That was included as a warning to society of the importance of protecting computerised devices and systems (Koops, 2012, p. 13; Koops, 2010, p. 3). Amongst the activities rendered unlawful under CC I, were hacking, spreading of viruses, wilfully corrupting data, intercepting data traffic without authorisation and forging bankcards.[14] The act also introduced a number of new investigative powers for law enforcement agencies, including the ability to intercept data and to obtain warrants ordering the disclosure of data, to gain access to computers and to conduct network searches. However, it should be noted that it is difficult to issue these orders to suspects, as no suspect can be forced to cooperate in their own incrimination.[15]

In 1999 a second Computer Crime Act (CC II) was tabled in Parliament. That move coincided with the development of the Convention on Cybercrime (CoC) by the Council of Europe, with the aim of creating a common legal framework in order to

[13] This is also referred to as digital crime.

[14] See DCC Articles 138ab, 138b, 350a and 350b, in conjunction with Article 80.

[15] See Article 125i-o DCC and see Article 6 ECHR

tackle this form of criminality at the international level. Since the Internet and computer networks have no borders, it is essential that states cooperate in fighting cybercrime.
As many of the activities covered by the Convention had already been outlawed under CC I, the Netherlands largely complied with it as drafted. Because one of the goals of the CoC is to harmonise its signatory states' national criminal and procedural law in the field of cybercrime, one of its most important aspects is cross-border access to computer data. In order to prevent breaches of national sovereignty in this respect, the Convention incorporates two exceptions whereby mutual permission is granted to take enforcing action. The first covers access to publicly available computer data and open sources, although this does not mean that Dutch law enforcement agencies are free to investigate such sources at will. When systematically gathering information about individuals, whether or not it comes from open sources, they must comply with Article 126 DCCP, which requires the investigative judge to set clear investigative parameters (Stol et al., 2012, p. 29-30).

The second exception concerns cross-border network searches. In principle, it is permissible to access data held on another computer system through a computer that is being searched. When that secondary system is located outside the jurisdiction of the investigating agency, however, then the consent of the person or entity authorised to disclose the data it holds is required (Kaspersen, 2006, p. 21). Although alternatives have been discussed, as yet the parties to the Convention have failed to find a way to enhance international co-operative arrangements in this respect.[16] Consequently, there remains a strong emphasis upon 'mutual aid' and a formal request for assistance always has to be submitted before any transnational investigation can take place. Koops and Goodwin point out that a non-consensual cross-border search or a direct order to foreign service providers would potentially be most effective for cyber investigations, but those ways are currently not permitted (Koops & Goodwin, 2014).
The Netherlands signed the Convention on Cybercrime on 23 November 2001 and it was ratified by the Government on 16 November 2006. As of June 2016, it has been signed and ratified by a total of 49 states.[17] Next to most of the members of the Council of Europe, they include important nations such as the United States, Canada, Japan and South Africa (Kaspersen, 2004).

The CC II entered into force in the Netherlands in 2006. This act was clearly influenced by the European Convention on Cybercrime, bringing a number of previously unharmonised matters into line with its provisions. One of the most important changes it made was redefining 'computer trespass' or hacking. The security requirement included in Article 138a DCC (old), meant that some form of protection had to be breached in order for this to constitute a crime. As stated earlier, the idea behind that provision was to highlight the importance of system safeguards. Consistent with the CoC, the new and still current Article 138ab DCC focuses on the intent underlying an intrusion and less on whether or not hackers know that their actions are unlawful.[18] Other new measures included criminalising denial-of-service

[16] *Convention on Cybercrime*, par. 193. http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CL=ENG.

[17] http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CL=ENG.

[18] This is also known as the 'colourless concept' in Dutch criminal law. The use of the word 'and' (*en*) separates the notion of 'intent' (*opzet*) from the 'unlawful' (*wederrechtelijk*) aspect, making it irrelevant whether or not the perpetrator was aware that they were breaking the law. In such cases it is assumed that they must know that their acts were unlawful and so that awareness does not need to be proven in court.

(DoS) attacks and the installation of viruses and malware. Also in line with the CoC, the CC II extended the legal definition of child pornography and made its production, possession or distribution in any form illegal.
The global, borderless nature of the Internet means that cybercrime is not confined by national frontiers. Its rapid online development constantly offers new ways to commit offences remotely, automatically and with multiple victims (Koops, 2012, p. 9), in a manner that often raises jurisdictional questions. The principal applied in the Netherlands is that of 'computer-based jurisdiction', with the geographical location of the server – or other 'computerised device or system', determining which jurisdiction is applicable (Klip, 2000, p. 140). In effect, this means that law enforcement agencies cannot do anything if the server is outside the Netherlands.[19] To put it another way, Dutch cyber jurisdiction ends at the nation's borders even though the Internet knows no frontiers. This principle is all the more remarkable because data can be used in investigations and any evidence obtained is admissible in court when the location of the server is unknown, yet a formal request for assistance to authorities abroad must be submitted as soon as it is found to be outside the country. How this system is supposed to work in practice has never been explained clearly in any of the official explanatory material issued for the legislation.[20] The great drawback of having to submit requests for assistance is that they can delay an investigation considerably. Especially in the case of cybercrime inquiries, this can have a huge impact on the final outcome.

Third Computer Crime Bill
In many respects, the CC II is already out of date. This is why in May 2013 a draft third Computer Crime Bill (CC III) was published.[21] This would introduce a number of far-reaching investigatory powers. In December 2015 the proposed CC III was presented in the House of Representatives. What's more, following the advice given by the Council of State,[22] the new draft will have stricter privacy guarantees. Consequently, the bill has been adjusted on a few levels. As mentioned, the bill will introduce new powers, including two designed specifically to help the Dutch law enforcement agencies in their fight against cybercrime. They are the right to gain remote access to computers, and the so-called 'notice and take down' (NTD) order. The accompanying Explanatory Memorandum lists three reasons why the government believes these new measures are needed: (1) the widespread encryption of electronic data; (2) the growing use of wireless networks; and (3) the application of cloud services. All of these have been hindering police investigations.
The accompanying Explanatory Memorandum states that the increased use of encryption for electronic communications (1) makes it essential for law enforcement agencies to be able to examine the underlying devices and systems directly, so that data can be captured before it is encrypted. In other words, they need the power to 'tap' the source used by the suspect, be that a computer, telephone or other device. As for wireless networks (2), they are considered a problem because network switching makes it more difficult to track a suspect's movements and activities. And the growth in cloud services (3) means that less data is actually being held on suspects' own devices. Since the majority of these services are based abroad, they currently cause jurisdictional problems and necessitate time-consuming formal requests for assistance (See also: Koops & Goodwin, 2014). Below we describe the

[19] Article 125j DCCP. On extraterritorial searches, in principle not permitted, see Wiemans (2004, p. 152-162).

[20] *Kamerstukken II* [Dutch parliamentary document] 2004/05, 26 671, no. 10, p. 23.

[21] A preliminary concept was also published in 2011. See: Oerlemans (2012). https://openaccess.leidenuniv.nl/handle/1887/17770

[22] *Kamerstukken II* [Dutch parliamentary document] 2015/16, 34 372, no. 4.

proposed new powers in more detail in order to provide a first impression of what the government hopes to achieve by introducing them.

The power to gain remote access to computers finds its legal basis in the proposed Article 126nba DCCP. This would allow the police to monitor suspects' activities prior to the encryption of data. After remote access is obtained to a device, the police would be authorised to carry out numerous operations, from establishing the suspect's identity to extracting data and observing it systematically. The remote access as an investigative power would only be permitted if this is in the 'urgent interest' of an investigation and with a warrant issued by the Public Prosecution Service and endorsed by the investigative judge. The term of such a warrant would be limited to four weeks, although it could be extended by further four-week periods upon application. In addition, the Council of State has deemed it fit to ensure that the police are only allowed to use this measure in case of serious criminal offences with a minimum prison sentence of eight years.[23] There are, however, exceptions to be made when there are social and economic interests at stake. One could think of a DDoS-attack on a bank or when fighting a botnet. A governmental decree will define these exceptions.
The other method is the 'notice and take down' (NTD) order, described in the proposed Article 125p DCCP, which complements the existing Article 125o DCCP to provide a legal basis for injunctions requiring Internet providers to deny the public access to certain material. This could range from an illegally posted file to an entire website. Yet, that sounds easier than it actually is: once on the Internet, material can never be entirely removed. Even after it has been deleted in one place, it can reappear somewhere else. In any case, the NTD order should be regarded as a provisional measure. Ultimately, it is up to the courts to decide what should happen to any information that is taken down.

The new version of the bill also pays more attention to other issues, such as information theft. In cybercrime cases, stolen credit card information or login codes to compromised accounts are quite regularly sold on the Dark Web. The offence will be punishable by a one-year prison sentence as a maximum sentence. Considering e-commerce is growing rapidly, it appears imminent that this will lead to scams. The Explanatory Memorandum states that the National Internet fraud Reporting Centre of the Dutch police received a total of 7.9 million euros worth of Internet fraud claims in 2014.[24] This new bill therefore proposes that the repeatedly offering of goods and services without actually delivering them will also become a criminal offence. It is suggested to make this crime punishable by four years prison sentence as a maximum sentence or a fine.

Code of Criminal Procedure
The investigation, prosecution and punishment of crime in the Netherlands are governed by the Code of Criminal Procedure, which describes the procedures for dealing with various categories of offence. It also details the rights of suspects, for example, the right to a legal representative of their own choosing (Art. 28, Clause 1 DCCP) and the right to silence (Art. 29, Clause 1 DCCP). The code also incorporates a number of the principles defined in the European Convention on Human Rights, such as the right to a fair trial and to a hearing within a reasonable time. Other topics covered include pre-trial procedures, applicable sentences, the examination

[23] Article 126nba(1c) DCCP.

[24] *Kamerstukken II* [Dutch parliamentary document] 2015/16, 34 372, no. 3, p. 72.

of witnesses in court and the admissibility of evidence, as well as recourse to appeal, judicial review and so on.
In addition, the DCCP regulates the use of certain far-reaching powers in the investigation of serious crime. This section of the code is commonly known as the Special Investigative Powers Act.

Special Investigative Powers Act
The Special Investigative Powers Act entered into force in 2000,[25] extending the means available for investigating organised crime by defining when and how the Dutch police can make use of covert methods. Because these are specific powers, the Special Investigative Powers Act forms part of the DCCP, namely sections IV to Vb. The powers concerned are: (1) systematic observation; (2) infiltration; (3) pseudo purchases; (4) systematic information-gathering; (5) sneak-and-peak operation; (6) electronic interception of communications; and (7) interception of private communications (Beijer et al., 2004, p. 277).
When considering the use of these special powers, the principles of proportionality and subsidiarity must be taken into account. Proportionality means that the use of an intrusive method has to be justified by the seriousness of the crime under investigation, and is reflected in the restrictions on the types of offences for which special powers may be authorised. For example, telephone taps are permitted only when investigating crimes defined in Article 67, Clause 1 DCCP (one carrying a penalty of at least four years' imprisonment) and when the crime, by its own nature or by virtue of its connection with other offences committed by the suspect, represents a serious violation of the rule of law (Art. 126m DCCP). The same requirement applies to infiltration, when a law enforcement officer joins or assists a group of individuals reasonably suspected of planning or having committed serious crimes (Art. 126h DCCP).
The proportionality of an investigative method is assessed twice. The first assessment is when the investigating team consults the public prosecutor on the proposal to use the method. In the first instance, it is the public prosecutor who determines whether it is proportional, but this decision must be upheld by the investigative judge in the form of an authorisation to actually deploy the method in question. In the case of 'milder' Special Investigative powers, however, such as retrieving historical data-traffic information, it is not necessary to obtain the investigative judge's consent.
The investigative judge considers whether the public prosecutor's request is reasonable in the sense that it complies with the principle of proportionality. The public prosecutor is also required to check its subsidiarity – whether the goals of the exercise could be achieved through less intrusive means – before this aspect, too, is reviewed by the investigative judge. The fact that these methods are specifically regulated by the DCCP reflects that they intrude on a suspect's privacy more than would normally be permissible.
When it introduced special investigative powers, Parliament allowed their use in the digital domain as well as the physical world. However, the scope of their applicability in that domain has not always been explicitly defined, sometimes leaving detectives unsure as to what exactly they are and are not allowed to do. This is the case, for instance, with so-called 'remote searches'. In a memorandum to Parliament, the Minister of Security and Justice has stated that such searches are permissible, subject to authorisation by an investigative judge, under Article 125i DCCP.[26] In prac-

[25] For an extensive description, see, for example: Krommendijk, Terpstra, and Van Kempen (2009).

[26] *Kamerstukken II* [Dutch parliamentary papers] 2014-2015, 286. https://zoek.officielebekendmakingen.nl/kv-tk-2014Z14361.html

tice, though, it seems that they are carried out only occasionally.[27] What is more, there is no literature that suggests the DCCP provides a legal justification for hacking as an investigative power (Koops & Buruma, 2007; Oerlemans, 2011).

Nonetheless, special investigative powers – in both their online and their offline variants – play a major part in the detection of cybercrime. Under Article 126m DCCP, for instance, it is possible to apply for permission to intercept Internet traffic. In 2010, the first year for which the Ministry of Security and Justice released the relevant data (Odinot et al., 2012), such permission was granted on 1,704 occasions. And in subsequent years, the number of 'taps' rose quickly, reaching 3,301 in 2013. The main reason for this increase was the growth in the number of smartphones in use, which can only be monitored effectively with both IP and telephone taps.[28] To put the figures into some perspective, the number of authorised telephone interceptions rose only modestly, from 25,487 in 2012 to 26,150 in 2013.[29] Since 2014, no distinction has been drawn between telephone and Internet taps – only the number of connections being monitored is counted. The combined number of taps totalled 25,181 in 2014.[30] In any case, intercepting voice communications can be just as useful in the investigation of cybercrime as tracking Internet traffic. As can other Special Investigative powers, such as systematic observation, infiltration and the installation of devices to eavesdrop on 'offline' conversations. But it is not known how often these methods are used each year.

Data Retention Directive

Until recently, if during an investigation police wanted to know where a mobile telephone was at any given moment and who it was calling, or who uses a particular IP address, they could obtain that information under the Data Retention Act. This was the implementation of the 2006 European Data Retention Directive, enacted to ensure that certain telecommunications and Internet usage information was kept so that it could be made available to law enforcement agencies investigating serious offences, including cybercrime. In 2012, the Research and Documentation Centre of the Ministry of Justice conducted a comprehensive study into the practical utility of these requirements for crime investigation purposes (Odinot et al., 2013). This revealed that historical telecommunications traffic and geolocation data was being requested and analysed on a huge scale, particularly in order to map social networks and to localise mobile telephones. It was also possible to use the data to determine when a computer or mobile device had accessed the Internet and, in the case of fixed-line connections, who their registered user was. All of which made a very valuable contribution to detective work.

Critics of the European directive claim that it infringed on personal privacy, and is at odds with Article 8 of the European Convention on Human Rights and Article 7 of the Charter of Fundamental Rights of the European Union. The European Court of Justice eventually agreed, and in March 2014 declared the directive invalid.[31] Questions were also raised in the Netherlands over the value and need for the national Data Retention Directive. Following on from the European judgment, on 11 March 2015 the Dutch implementation of the Directive was struck down by a Dutch court.

---

[27] See Rechtbank Rotterdam [Rotterdam District Court], 26 March 2010, LJN BM2520, and Hof 's-Gravenhage [The Hague High Court], 27 April 2011, LJN BR6836.

[28] *Kamerstukken II* [Dutch parliamentary papers] 2013/14, 33 930 VI, no. 1, p. 50.

[29] *Kamerstukken II* [Dutch parliamentary papers] 2013/14, 33 930 VI, no. 1, p. 50

[30] *Kamerstukken II* [Dutch parliamentary papers] 2013/14, 33 930 VI, no. 1, Appendix, p. 17.

[31] http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054nl.pdf.

As a result, telecommunication providers no longer have to retain data for a set period. The Public Prosecution Service (Ferdinandusse, Laheij & Hendriks, 2015) has expressed concerns over this development and its likely repercussions for detecting cybercrimes and other offences. Certainly in the case of Internet-related crimes, it is quite common for a suspect not to be identified until sometime after the committed crime. This is why investigators consider it essential that certain 'old' data remain available to assist them in their inquiries (Ferdinandusse, Laheij & Hendriks, 2015, p. 41). Even the civil court which annulled the law stated that scrapping the data retention 'could have far-reaching consequences for the investigation and prosecution of criminal acts'.[32] The Council for the Judiciary too, in a legislative recommendation issued in February 2015, stressed the importance of such a requirement[33] whilst at the same time acknowledging the need to protect people's basic rights. It therefore proposed a system whereby any application to force the disclosure of telecommunications traffic data would require the assent of an investigative judge.[34] Quite obviously, the political debate on this issue is far from over. Law enforcement agencies can still request data since the annulment, but without the retention requirement the results of any such application are entirely dependent upon the provider. Providers are free to decide what information they keep, and for how long.

Research showed that in 2012, a couple of years before the retention rules were struck down, a total of 56,825 applications were lodged to obtain historical telecommunications traffic and geolocation data subject to those rules for analysis. That information was thus widely used in criminal investigations. The police inquiries into the cases reviewed for this study were all conducted while the rules were still in force, so the invalidation of the Data Retention Directive and its consequences were not under discussion.

[32] Rechtbank Den Haag [The Hague District Court], 11 March 2015, ECLI:NL:RBDHA:2015:2498, r.o. 3.12.

[33] Letter from the RvDR, 2015.

[34] Ibid.

3 Characteristics of cyber-OC

3.1 General description of the cases

This study is based on an analysis of the police files of eleven criminal investigations into cyber-OC. Of the eleven investigations, ten were handled by the NHTCU. Three cases were entirely national in nature: the suspects were located in the Netherlands and the great majority of the investigative work took place within the country. Some information was requested from abroad, for example, data held by hosting providers, car hire firms and telecommunication services. In the remaining cases, the crimes had an international character. Only one case was carried out at district level. This was a case in which web shops were hacked and goods fraudulently ordered on behalf of existing clients. The delivery addresses and the residences of the group responsible were all concentrated in one geographical area in the Netherlands, and the suspects were acquainted with one another as members of the same ethnic community. In this case there was no co-operation with foreign law enforcement agencies.
The fact that only one of the selected cases was dealt with at district level is a consequence of the focus of this study: cyber organised crime. The 'organised' crimes are regularly tackled at a national level within the police organisation. In the Netherlands, the required expertise is concentrated in the NHTCU, which operates at the national level and works regularly with law enforcement agencies in other countries.

Case descriptions
The eleven cases examined pertained to distributing malware, hacking, running botnets, phishing, abusing the banking system, money laundering and illegal online trading. Below the cases are described briefly.

Case 1: A group from Romania succeeded in hacking a bank's two-step customer identification process and was able to manipulate bank cards and payments. Cash totaling approximately 1 million euros was withdrawn all over the world. The case file names twelve suspects, although a large number of unidentified individuals also played a role. Operating from the Netherlands, the gang is not particularly tight-knit and various members are also active in 'traditional' crime, either individually or in small groups.

Case 2: A group of nine Dutch suspects used malware to steal money, and then attempted to launder it using numerous 'mules'. An investigation was initiated after a number of Dutch banking institutions lodged formal complaints with the police.

Case 3: Two Dutch hackers broke into the network of a Dutch law firm. This offence falls within the 'narrow' definition of cybercrime, although the suspects are linked to traditional organised crime in the Netherlands.

Case 4: Botnets were constructed, maintained and rented out on a large scale. Although only one suspect has been identified, there are indications that he was not acting alone. The systems discovered were so extensive that they could not have been managed and maintained by a single person. The dozens of servers used were financed by other, as yet unknown conspirators. The suspect's proceeds from these activities were considerable, with estimates ranging from € 100,000 to € 180,000 a month. This was a technically complex form of cybercrime.

Case 5: This case concerned a major DDoS attack, which disrupted large parts of the Internet. Interestingly, the motive behind this crime was the issue of who makes the rules and laws governing the Internet, and so ultimately who controls cyberspace. One Dutch suspect is currently being prosecuted in the Netherlands and a juvenile has already been convicted in the UK. There are indications that those responsible were in contact with others in a number of countries, who may also have taken part in the attack and so enhanced its severity.

Case 6: Ransomware was distributed in the Netherlands and other parts of Europe. An infected computer was 'locked', with the victim seeing a message that, for example, child pornography had been found on it and that the machine would only be 'unlocked' upon payment of € 100. These notifications used the logos of law enforcement agencies in the country concerned. The suspects were also active in money laundering. Three suspects are currently being prosecuted in the Netherlands.

Case 7: A large group of Surinamese suspects was smuggling drugs into the Netherlands through a port, by stealing the containers used to transport the drugs. In order to enable the gang to steal the containers undetected and return them unnoticed, the port's computer system was hacked. Thirty-four suspects are being prosecuted in this case and another 14 individuals have been linked to it but, for various reasons, are not facing charges.

Case 8: Computers and mobile telephones were infected with banking malware. The suspects responsible targeted mobile banking customers of a large Dutch bank, who were sent an e-mail containing a link to a fake website on which they had to enter login details. They then received a text message encouraging them under false pretenses to install a malicious app on their mobile telephone. This enabled the suspects to intercept text messages from the bank and finalise money transfers.

Case 9: After committing credit card fraud and hacking offences, two Dutch hackers got into an argument with the owners of two websites, which were then briefly subjected to DDoS attacks.

Case 10: An organised criminal group offered and supplied drugs and weapons through a market on the dark web. They were also involved in setting up their own illegal online marketplace. Although those responsible are thought most probably to be Dutch, their activities extended as far as Sweden, Belgium, Germany and the United Kingdom. Several suspects were arrested almost simultaneously in February 2015, and the server hosting their own website was seized.

Case 11: A group of suspects succeeded in obtaining details of clients of major Dutch webshops through phishing. Goods were then ordered in their names, but diverted by complicit couriers so that the victims were unaware of the fraud. The items were subsequently sold again.

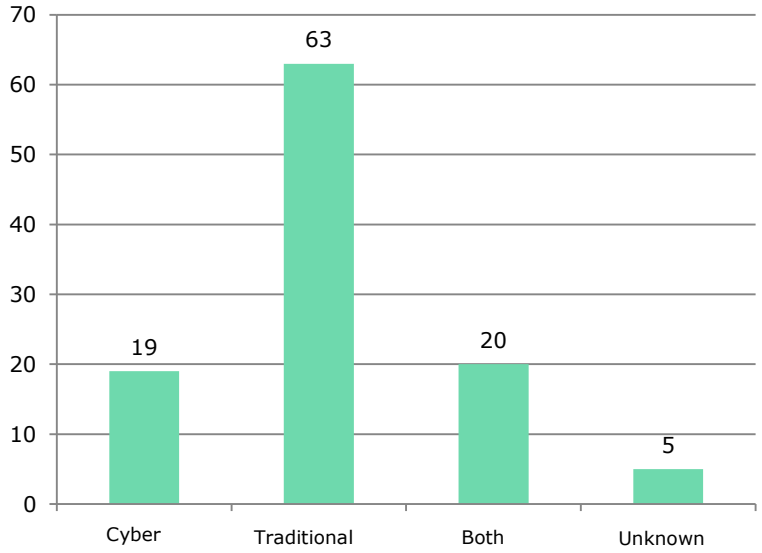
3.2 Suspect characteristics

Suspects in the eleven cases

Overall, 107 suspects are described in the eleven case files studied. Almost all (102) are male, with the five females confined to just a couple of cases. Thirty-nine were involved directly in cyber criminality, with half (20) of these also known to be active in other types of crime. Another 63 suspects were implicated in the cyber-OC inves-

tigations, but their own activities were not particularly ICT orientated. The role of 5 suspects was unknown.
In terms of background, the suspects are a highly diverse group. Some are university educated, some qualified IT specialists and some have only had a secondary school education. Others run their own businesses, are working or studying, or are unemployed, drug addicts and homeless. Most (75) are Dutch nationals, but some come from Romania, Ghana, Surinam or other countries.

Figure 1 Suspects by primary role



Age
Many people think of the typical cybercriminal as young and technically skilled (Dietrich et.al., 2016). According to the Deputy Head of the UK's National Cyber Crime Unit, quoted on the website dutchcowboys.nl,[35] offenders often try to recruit youngsters with IT skills for illegal activities through online forums and discussion boards.

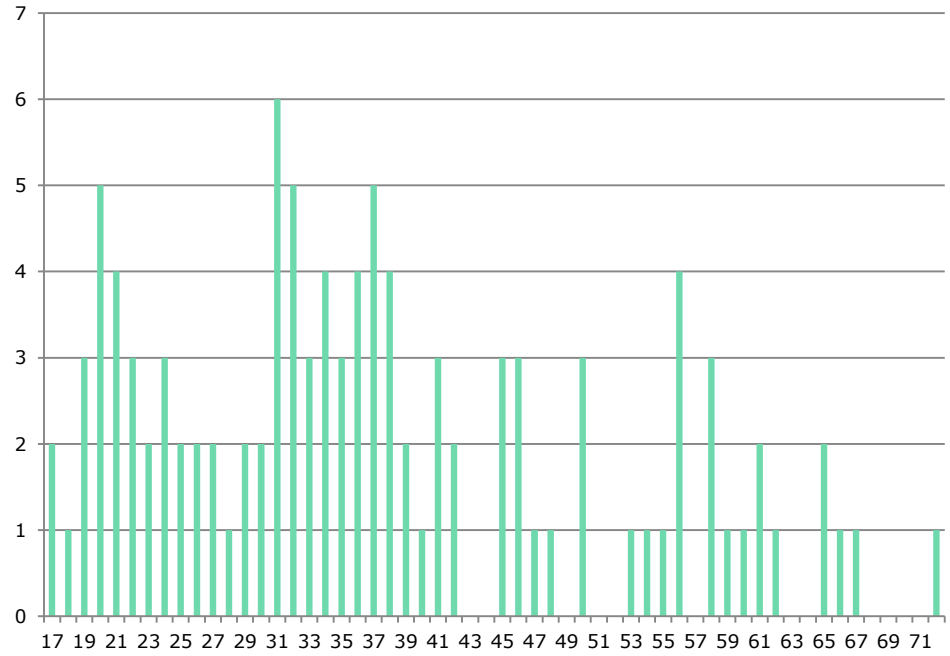
> *'More and more teenagers are becoming wired in to a digital environment from an early age, acquiring potentially dangerous skills such as coding and hacking. Technology chat rooms and posting boards are the perfect place for criminals to scout the next generation of highly skilled teens. We need to bear in mind that kids can easily be lured into the world of cybercrime. Often, they are not even aware themselves that they are involved in illegal activities.'*

Reports like those about a 17-year-old who hacked a large Dutch telecommunications provider and a London teenager responsible for a DDoS attack at a very large scale, at the age of 16 or 17, only serve to reinforce this image. Other studies, however, reveal that cybercriminals are not necessarily teenagers (Detica/BAE Systems 2012). This finding may not be as contradictory as it seems, though, because it is also possible to start young and to remain criminally active later in life.

[35] Retrieved from www.dutchcowboys.nl/cybercrime/politie-en-cybercriminelen-zijn-op-zoek-naar-medewerkers-met-dezelfde-vaardigheden; accessed July 2015.

The ages of the suspects in our cases ranged from 17 to 72 years. Their mean age was 37, although the 39 suspects whose individual activities concern ICT orientated crime were slightly younger, averaging 29 years.

Figure 2 Suspects by age



Criminal histories

We do not know the criminal histories of all 107 suspects, but almost half (49) are known to have previous convictions. These range from drug offences to fraud, violence and hacking. Almost a third of the 107 suspects were not previously known to police. As explained earlier, within the studied cases some are suspected of purely technology-based cybercrimes and others of more traditional, non-technological offences. The former category includes using malware and botnets, hacking systems, deploying remote access tools or carrying out DDoS attacks, whereas the latter encompasses supporting activities like fitting skimming devices to cash machines or laundering the proceeds of cybercrime. It also covers intermediary roles such as recruiting money mules or front men for operations, as well as 'mainstream' offences such as drug smuggling or theft.

Of the 'pure' cybercrime suspects, only three had previous convictions for computer-related offences but six had records for other criminal acts, such as burglary, theft or drug crimes. Eight had no criminal history, and in two instances criminal history could not be ascertained from the case files.

Figure 3 Suspects with criminal history

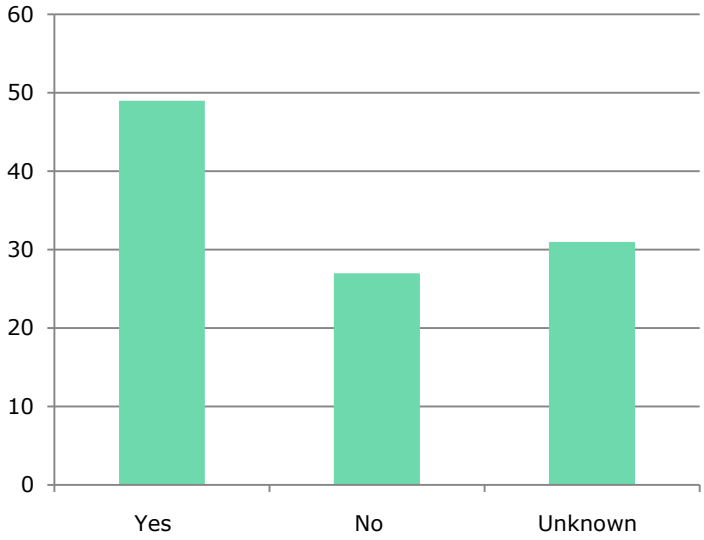
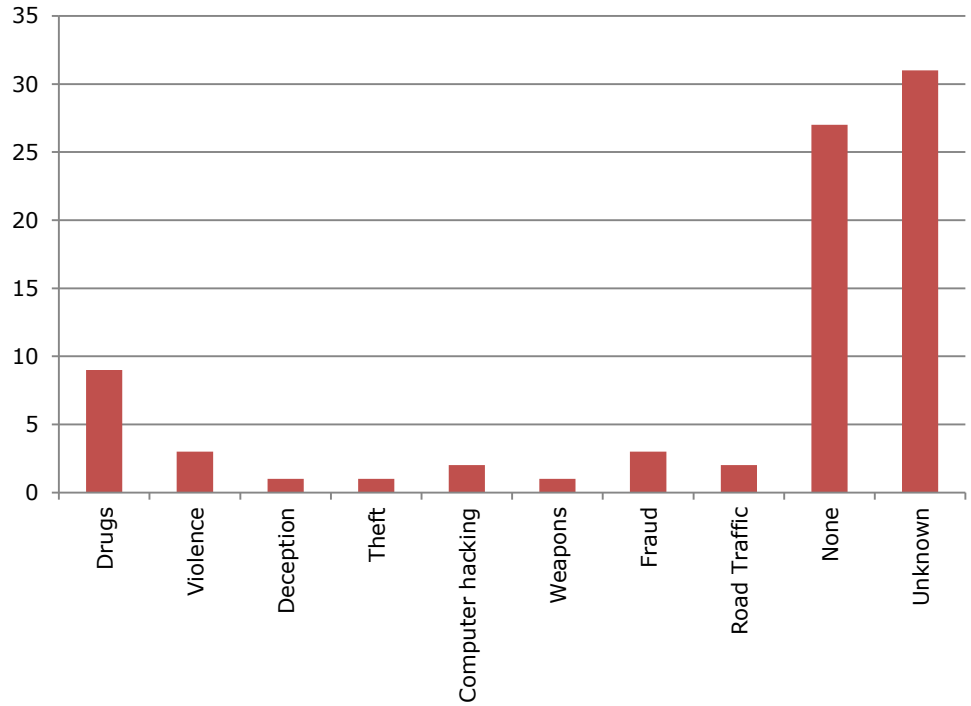


Figure 4 Criminal history of suspects



Motives

In order to understand and address organised cybercrime and to compare this with other forms of organised crime, it is important to know what motivates the suspects. In this respect, the suspects themselves are a key source of information. A number of the case files we looked at, provided some insight into this aspect of their

crimes, either in statements made to the police or from intercepted conversations or chat sessions. We did not speak directly with any offender or suspect for this study, but the files reveal a variety of motives:

- making money;
- paying off large debts;
- disputes or revenge;
- persuaded or forced by others;
- as a hobby.

Motives can also overlap. For example, activities may start out as a hobby but develop into a serious crime when the suspect realises there is big money to be made. One suspect asserted that hacking websites was an innocent pastime, although international press reports on his case indicated that he and his accomplices had netted millions of dollars from building and renting out botnets to distribute malware and spam.

While some fantasise about making a fortune with their computer skills, there are also suspects who received only small sums for providing particular services. These might include opening a bank account, allowing suspects to use a bank card or account or signing for deliveries ordered fraudulently. In one case, mentally unstable people and people with additional problems gathering at a well-known hangout were pressured into signing Chamber of Commerce forms to put businesses in their name, in return for a few euros. And several of the suspects in this case, in which money was stolen by breaking into an online banking system, had already existing large debts. The same applied to one of the other cases – another scheme to defraud banks.

As well as money and debts, *disputes* also provide a motive to commit cybercrime. One case, for example, centred around an argument over a family inheritance. One of the family members involved called in a couple of computer-literate acquaintances to hack the systems of the law firms handling the matter, in order to obtain documents concerning the sharing of the inheritance. Whilst money certainly played a role in this case, the primary motivation behind the crime was the family dispute. As far as one can ascertain, the youngsters responsible for the actual intrusion were not paid for their part in the affair. They seem simply to have wanted to help, although their 'patron' did pay for the necessary software.

We encounter a similar motive in another case, which has its roots in an argument between two hackers and the owners of two websites. At least in part, the argument was about the publication of personal details of a girlfriend on one of the sites. The hackers subjected the sites to DDoS attacks as a form of retaliation.

In some cases people are induced or persuaded into criminal acts, such as developing malware, possibly even without knowing its intended use. In one case, for example, two suspects were first coaxed and later blackmailed into producing malware, which was then used to hack a logistics system so that drugs could be smuggled into the country.

The motive behind an offence is not always clear. The suspects in another case apparently used a DDoS attack as a form of protest against the prominent market position of a large anti-spam firm. Their driving force seems to have been related to power, some kind of dispute and what they regarded as 'injustice'. We also see suspects whose main purpose is to show off what they are capable of. In their keenness they find themselves breaking the law, or at a certain point feel that they are unable to turn back.

In the files, we also found a handwritten letter from a suspect. It was written in jail and addressed to the judge. It contained the story of how he got involved in the organization. He wrote that he should have known better and that he regretted his involvement in the organization. His letter gives a rare insight into how this person reflects on his motive to help the criminal organization;

> *'I saw [building] the website as an assignment, nothing more than that. That job developed gradually. We never spoke about the content of the website. I was not interested in that aspect. For me, it was all about the technical part and the challenge. And by that, I do not mean the challenge or excitement of doing 'bad' things. The challenge was building a technical application that worked perfectly.'*

In more general terms, a police officer said the following about the motives behind cybercrime:

> *'As with other types of crime, the motive for most offenders is money. Although there are sometimes those who say they do it for fun or out of boredom, or for power on the Internet.'*
> – Police interviewee

The literature on this topic also reports a variety of motives. In their review, Van der Hulst and Neve (2008, p. 22) found that a substantial proportion of high-tech crimes are financially motivated. But many hackers and malware authors, in particular, have more diverse reasons for engaging in their criminal activities: the challenge, ideology, power, revenge or vandalism, for example. Europol (Europol, 2003 in Van der Hulst & Neve, 2008, p. 87-88) has distinguished the following motives for high-tech crime:

- personal advantage, for example in the form of useful information, financial gain or avoiding payments;
- political convictions, including personal, ideological or moral views;
- curiosity;
- mischief and vandalism;
- harassment;
- desire for power.

In short, money seems to be the primary force behind cybercrime, but a host of other motives also play a part. Our cases confirm these findings.

3.3 Activities and modus operandi in the field of cyber-OC

Cybercrime and the Internet as target, tool or space
The suspects in our selected cases were active in a number of different forms of cybercrime: distributing malware, hacking, running botnets, phishing, abusing the banking system, money laundering and illegal online trading. Some focused on one particular activity and others on several at the same time. In this section, we examine these activities in more detail, as described in the police case files. Since activities are often combined, it is difficult to look at an individual modus operandi in isolation.

Malware
A number of suspects were in possession of malicious software (malware) that can be remotely installed unnoticed on other people's computers. This potentially gave

them access to private computers or sensitive personal information, or allowed them to block the devices remotely. Depending upon the extent of their own technical expertise, suspects either developed this malware themselves or acquired it from others.
For this reason, the files do not always reveal the actual writers of the malware. In another case, however, they were identified by police. However, it should be pointed out that the suspects continue to deny their role in this crime. Using phishing e-mails, these individuals installed the banking trojan TorRAT on victims' computers. That gave them remote control over the infected devices and enabled them to manipulate the Internet browser. In order to perform spam runs, they used servers they had also accessed illegally. Research by the ICT-security company Fox-IT revealed that TorRAT had been developed by the criminal organisation itself[36] specifically to target customers of Dutch banks. Its functions included altering data in the online banking environment; for example, to make clandestine extra payments or modify actual transactions and so divert funds to the suspects. In order to mislead investigators, they rolled out a second program, 'ZeuS banking malware', at the same time in the hope that forensic specialists would focus upon that rather than TorRAT.
In most of our malware cases, however, the suspects used software they had obtained from others. But for some this helped them learn more about what malware looks like and how it works, so that they could perhaps develop their own.
In one case, a suspect was sent malware by its maker through a website for exchanging large data files. After his arrest, the recipient told the police that this method was used to distribute the programme to people in different countries for their own use. This particular case involved a specific form of malware – ransomware – which effectively 'kidnapped' the victim's computer by encrypting certain files to make them inaccessible. Other forms of ransomware 'lock' the entire device, so that the victim is unable to use it at all. Either way, the aim is to extract a ransom. Once this has been paid, the victim is sent a code to reverse the encryption or unlock the computer. At least, that is what they are promised. There are no guarantees, of course. The suspect in one of the cases used advertising websites to spread the ransomware.
In another case, Dutch suspects with little or no IT experience of their own hired foreign computer specialists to develop malware on their behalf. This malware infected victims' mobile telephones as well as their computers. They were sent a link, supposedly by their bank, asking them to install what was actually a malicious app on their phone. The app surreptitiously forwarded text messages to the suspects, allowing them to intercept verification codes from the bank and so perform illegal transactions. The investigation in this case never identified the actual writers of the malware.
In all the malware cases we studied, computers and the Internet were used as *tools* in crimes committed for financial gain.

Hacking
Hacking is a way of gaining unauthorised access to a system. It can be regarded as a pure form of what Dutch law defines as 'computer trespass'. Unlike a malware infection, which installs malicious software on a large number of devices, hacking is a focused intrusion into a specific system or network. In other words, the computer itself is the *target*. Since hacking is a fairly broad term, however, it can cover various forms of activity. One is the use of so-called 'exploits', which take advan-

[36] Retrieved from http://computerworld.nl/beveiliging/79823-torrat-bende-anoniem-door-gebruik-vpn-en-bitcoins, December 2016.

tage of security leaks in software. Special 'exploit kits', on sale in underground marketplaces, enable whole series of leaks to be misused – to place malware, for example.
Such a kit was part of the modus operandi in one of the cases. Computers were infected when their users visited a manipulated website with a particular URL. Its server was running an exploit kit, which quickly checked the visiting devices for security leaks: for example, outdated versions of Java containing vulnerabilities that provided a way to install the malware.
Malware itself can be used for hacking, too. This occurred in a case, which involved hacks of a law firm and other targets. The two suspects achieved this by sending out phishing e-mails themselves from a domain created especially for the purpose. Clicking on an embedded link installed a Remote Access Tool (RAT) on the computer, allowing the suspects to penetrate it in search of confidential information. In another case, a pair of hackers gained access to the computer systems of two companies in order to facilitate the passage of containers holding consignments of drugs through a port in Belgium. Their work enabled other members of the gang to collect the containers earlier than originally scheduled without attracting suspicion, and then later – once the drugs had been unloaded – deliver them to their original destinations.

Botnets
Botnets can be used to link multiple computers together. A botnet is essentially a network of individual malware-infected computers, which can be exploited remotely for various forms of illegal activity without their owners' knowledge. They are often used to distribute spam or to impede access to particular website by carrying out distributed denial of service (DDoS) attacks. In one case, the *distributor* of the malware made the computers he infected part of the botnet operated by its *maker*.
Another case was a joint enterprise by a group of suspects, each with their own specialism. These included developing malware and webinjects, managing botnets and laundering money. Infected computers in this case joined a botnet, which could then be used to collect details of their users' bank accounts. When victims tried to log into the online system of a major Dutch bank, they were redirected to a fake website. As well as their account number and passwords, this also requested their mobile telephone number and asked what type it was. A text was then sent, with a link to install an app. This infected the device with malware, which redirected bank messages containing transaction verification codes to the suspects.
In one of the cases, one suspects created several botnets, which he used both to distribute malware and spam and to carry out DDoS attacks. He also rented them out to other suspects for their own illegal purposes. Using the Bredolab virus, spread through advertising banners on a range of websites, this one individual was able to create a global network of some 30 million infected computers.
Another case centred on a prolonged DDoS attack on a non-profit organisation, lasting several days and involving more than 30,000 unique DNS resolvers – servers that couple domain names to IP addresses. One of the main suspects in this case passed on the necessary source code to accomplices through an online chat message. That code enabled the group, acting in concert, to submit large quantities of data to multiple DNS servers and so implement the denial of service.
As these examples show, with a botnet, computers are both a tool in the crime and the target.

Phishing
The cases described above reveal that suspects rarely use just one means to target their victims. This applies even more so when it comes to phishing, since that is

merely a technique for eliciting personal information for misuse in some other way. Over the years phishing e-mails have improved on many different levels. Currently, it proves to be difficult for consumers to distinguish a phishing e-mail from a legitimate e-mail message. It often takes the form of a fake e-mail message encouraging the recipient to click on a link and then enter private data, or initiate the installation of malware. Such methods are found in several of our cases.
In one of the cases we see an example of phishing. Using e-mail addresses stolen from an organisation, the suspect conducted a spam run consisting of messages in Dutch supposedly from large Dutch companies requesting the immediate settlement of an outstanding bill. Clicking on the 'final demand notice' attached to the e-mail installed malware on the victim's computer.
Another case also used fraudulent e-mails, apparently from a major Dutch online retailer. In this case, the e-mails contained a link to a fake version of the webshop, through which unwitting victims supplied the suspects with their log-in details. These were then used to alter delivery addresses and place orders, which were intercepted by the delivery couriers and delivered to the suspects.

Abuse of the banking system
A fifth form of cybercrime targets electronic payment systems. In one case, for instance, one person collected Dutch banking details using a botnet operated by someone else. The botnet operator has never been identified, but is thought to be in Russia. They used WebMoney to pay for each other's services. The person who originally gathered the information offered the same material for sale elsewhere too, on a forum for stolen data, and also bought credit-card details there to make purchases from online retailers.
Another case involved the skimming of bank cards. The suspects modified e-identifiers used by a major Dutch bank for online banking and fitted them to cash dispensers. This enabled them to 'skim' information from cards inserted into the machines and to add it to a database. From there, account numbers and PIN codes were loaded onto the magnetic strips on telephone cards and used to withdraw money abroad.

Other: laundering the proceeds of cybercrime
Various techniques are used to channel the proceeds of cybercrime to a 'safe' place. In one of the cases, a whole network of so-called 'money mules' was employed to make cash withdrawals in different countries, from various compromised accounts. Mules also feature in another case, where their role included routing funds to companies in the UK. International money transfer services are another favoured method. In one case in particular, a whole range of such channels was used: PayPal, Western Union, WebMoney, bitcoin exchanges and so on. Once the money had been moved abroad, much of it was used to buy luxury goods.
Finally, as in one of the cases, there are suspects who utilise the Internet as a platform or space for the perpetration of more conventional offences. In this particular case, a group moderated dark web marketplaces, and also sold drugs and weapons on their own website.

3.4 Counter strategies and shielding activities

In the movies, crooks wear balaclavas, buy guns from shady underworld dealers, pay in cash, drive cars with false number plates and disappear into the traffic when they make their getaway. In their own way, cybercriminals are no different. The case files we studied reveal plenty of different techniques they use in an effort to

conceal their identity, location and communications and keep their criminal activities under wraps. The digital environment of the Internet is very well-suited to such subterfuge, and the methods deployed in some of our cases proved extremely effective. At the same time, though, the fact that police managed to link at least one suspect to each crime shows that they were not always entirely successful. Moreover, in the studied cases investigators often managed to penetrate an entire criminal network or at least gain access to its communications. In this section we describe how suspects in our cases tried to protect and hide their identities, their substantive communications and their activities.

Concealing identities

Naturally, the suspects in our cases never use their full names on the Internet. Instead, they conceal their identities behind first names, personal nicknames or aliases borrowed from comic-strip characters and such, or simply random alphanumeric, such as 'a1987634tormail.org'. Several of the suspects in our cases had dozens of pseudonyms, each with its own e-mail addresses. Their online contacts often focus upon the exchange of information. In one case file, for example, we read how suspects worked together under aliases on preparations for a DDoS attack. The exchanges take place in chatrooms, accessed through anonymisation software so as to make it impossible to trace the traffic back to an identifiable individual. In several cases, Tor (The Onion Router) is used for this purpose. This tool facilitates anonymous surfing and access to websites, ending with .onion, on its own network which is invisible to a normal browser. Tor has become extremely popular in recent years, but is by no means the only anonymisation software encountered in our cases. Proxy servers are also used to disguise the IP address from which the Internet is being accessed. In one case, hacked computers were being exploited as proxies, thus protecting the suspect's own network and allowing him to operate anonymously. Hiding their source IP address also makes it impossible to tell where a person is. Other suspects used a Virtual Private Network (VPN) – a link that encrypts data, thus shielding it from prying eyes, and again does not reveal the visitor's IP address when he accesses websites.

Because of this anonymity, even the participants in a criminal conspiracy may not know who their online accomplices are. In one case we examined, a police interview with one suspect gave the impression that he had no idea that the person behind a particular nickname was actually a close associate of his in the real world, somebody he met and talked to regularly about criminal activities. In another instance, a suspect was surprised to learn that a partner in crime who had been arrested abroad was in fact a 16-year-old juvenile. From the nature of their online discussions, including his technical expertise and style of communication, he had formed the impression that he was in touch with a young man aged about 25. They had never met in person. The same applies to many of the contacts described in the files, particularly in cases of cybercrime in the narrow sense of the word. The individuals concerned form a purely online community, actively in communication on the Internet but total strangers to each other in the real world. Even commercial transactions within this community remain entirely anonymous. The prime suspect in one of our cases was actually seriously ill and confined to his bed for most of the day, although from there he was trading actively in drugs and firearms. But having adopted the name of a senior figure in the Sicilian mafia as his alias, his online alter ego went to some lengths to present himself as an imposing and dangerous figure.
In two of the cases we studied, all contacts between those involved were online; there is no evidence that they ever met. But this did not prevent them from transacting their criminal business, both amongst themselves and with clients. In the

other cases, however, besides online contacts and communication there were offline meetings as well.

The degree of technical sophistication with which suspects attempt to hide their location or identity varies widely. One, for example, believed that he was safe because he was using his neighbours' Wi-Fi network.

'My neighbours' computer – no-one can intercept that.'
– Suspect, excerpt from a chat session

In a case involving a DDoS attack on a website, the suspect recorded his actions and posted them in a video on YouTube. But in so doing, he overlooked the fact that his own face was visible in a photograph on his screen. Other suspects, however, are very deliberate and careful when it comes to protecting their identities. In another case, they always used pseudonyms and only ever communicated by TorMail. And even then they only referred to their activities in veiled terms. They mostly met in person; their accounting records were kept on paper and also featured only pseudonyms. The social control within this group was strong, too. One member was reprimanded when he sent a to-do list by ordinary e-mail.

'In future, never let this kind of info "loose" on the Internet.'
– Suspect, excerpt from a TorMail exchange

In this case, the suspects were very successful in concealing their identities and locations. It was only an anonymous tip-off tweeted to police which enabled them to gain access to the group's communications. Without that, our interviewees admitted, the case would probably never have been tried in court.

False papers
In three of the cases we studied, false identity papers were used to help conceal identities; for example, to rent a server under an assumed name. The costs were then charged to the accounts of firms that knew nothing about them. In another case, false papers were used to facilitate transactions at Bitonic – a service that buys and sells bitcoins. In the third case, both fake documents and fake personal data were used to register domain names from which spam runs were then performed.

Money mules
In 'traditional' financial crime, 'front men' are often used to conceal the true identities of those conducting illegal transactions. According to experts we interviewed, certain forms of organised cybercrime are conducted in much the same way. Often, so-called 'money mules' are used to hide the true nature of a transaction. Particularly with phishing and malware targeting the online banking system, they are a favoured way of converting the proceeds into cash. Innocent, often vulnerable people are pressured into letting people use their accounts in return for a small payment. Stolen money is deposited into these accounts, and the mule then either has to withdraw it in cash and hand it over to the criminal or transfer it into another account. The mules themselves are paid a trivial amount, but – often without realising it – are committing serious money laundering offences. Sometimes they are even duped into taking part; for example, by accepting an offer to work from home, which turns out to consist of receiving and transferring funds. The experts we interviewed say that investigations into organised cybercrime often hit a dead end with the money mules: the 'big fish' responsible for spreading or writing malware or

sending phishing e-mails are never traced by police. In one of our cases, mules were used to recover funds diverted from victims' accounts by the use of malware. In this instance, police arrested the suspected members of the core organisation, as well as many of the mules, partly thanks to an anonymous tip that gave them access to the group's internal communications. When they were arrested, a set of written accounts was also found. This provided additional evidence for the prosecution. In the transcripts of the intercepted communications, we read how the mules were recruited. The individuals were previously unknown to the person who found them, literally on a street corner, but were so keen to make money that they were prepared to make their bank accounts available and go together with the criminal to a bank or cash dispenser to withdraw the funds as soon as they were deposited. As much as € 9,000 was cashed in this way; the mule's cut ranged from € 75 to € 300.

A: 'So, er... we're talking about ten grand or so.'
NN: 'Yeah, uh… I don't know, not someone that soon.'
A: 'OK, uh… yeah...'
NN: 'Not within 20 minutes, I think.'
A: 'No, huh. I'll call you back, yeah?'
NN: 'Yeah, I think the church or somewhere, there's usually a couple there. But within 20 minutes, that I don't know.'
A: 'Yeah, it really has to be quick, quick you know, otherwise it's over.'
NN: 'Hmmm.'
A: 'I'll call you back, yeah?'
NN: 'Yeah, that's fine.'
– Excerpt from an intercepted telephone conversation

On one occasion, the suspects even took advantage of close relatives. Not only was the sister of one suspect used as a money mule, but also his girlfriend. She was asked to open a bank account in the name of the couple's son, to be used to channel stolen money. This, however, is not the best way for suspects to conceal their identity.

Protecting communications
Whenever people work together, they need to communicate in order to manage their activities and co-ordinate tasks. Some suspects are more successful at protecting their communications than others. The methods used range from veiled language to advanced security technologies.
The case files contain many examples of internal group communications. These include logs of prolonged online chat sessions between different individuals. The fact that the logs are in the files means that police gained access to suspects' communications at some point during their inquiry. Some of the conversations were of pivotal evidential value, as they provided an insight into the suspects' actions and tasks.

A: 'We need to find more people…'
B: 'OK, so we need recruits. I can handle that.'
– Excerpt from a chat log

Strikingly, we find that 'old-fashioned' telephone calls remain a widely-used means of communication. The files contain numerous transcripts of tapped calls. Some suspects seem completely oblivious to the fact that they might be overheard, freely discussing their affairs on the telephone. The transcripts include discussions about sharing proceeds, buying malware and plans to defraud customers of a particular bank.

D: 'Yeah, yeah, because they hadn't taken out everything that was in that container.'
T: 'No.'
D: 'No, no.'
T: 'Could be, could be...'
D: 'A hundred and ten kilos they left, lying there between the artichokes.'
T: 'That's there, too. Yeah, that's in the paper. Yeah.'
– Excerpt from an intercepted telephone conversation

In other cases, by contrast, the suspects are very aware that the police could be listening in. In one case for example, the central figures never communicated by telephone at all. They spoke only in person, or using encrypted channels. But others involved in this conspiracy, somewhat removed from the five main players, were not so careful and the police intercepted their communications.

In general, suspects do realise that the telephones may be tapped. Hence the many examples of veiled language we see in the transcripts. In one, for example, a number of 'girls' represented a particular quantity of cocaine and a 'party' was the departure of containers or a ship. This group also used plenty of jargon, such as 'traffers' for people responsible for Internet traffic, 'coders' for malware developers and 'ripping' or 'toppling' for swindling partners in crime.
In another case, the telephone was used only for brief conversations to confirm meetings. Nothing of substance related to the crime was discussed.

'My no., 0612 345678, is a subscription line, so say nothing on the phone – we'll arrange to meet up somewhere.'
– Handwritten note found during a police search of a property

Some suspects make deliberate efforts to frustrate police taps, such as using pay-as-you-go mobile telephones and changing them often. During one investigation, a large number of handsets and SIM cards were found during a search. Research (Odinot et al., 2012) has shown that switching cards and using unregistered pay-as-you-go phones is a tried and trusted method to avoid detection. And it is one also used by suspects in the studies cases.

'I get a new phone every time, and then I throw it away.'
– Excerpt from an intercepted conversation.

Moreover, it is apparent from the files that some suspects are aware of software, applications or devices which encrypt peer-to-peer telephone conversations. No transcripts of any such calls were found in the files studied, for the simple reason that they cannot be tapped. But in two cases suspects were overheard discussing the use of this technology.

N: '...And er, be careful. And this call is being tapped, you know that?'
J: 'Yeah, I know, I know. Shame you don't have an Android, you know, then I could have installed Redphone for you, then the call would be encrypted.'
N: 'Can't you do that, then?'
J: 'No, not with an iPhone, apparently. Only with Android.'
N: 'You think so?'
J: 'Yeah.'

J: 'At least with A I've got... when I talk to him on the phone, it's encrypted. Then no-one can listen.'
– Excerpt from a intercepted conversation

As well using the telephone, suspects also communicate extensively online. The Internet offers numerous ways to conceal the contents of an interaction, or the identities of those involved. People meet on forums on the dark web, for example, where the participants are untraceable, or sometimes in closed groups on Skype. The possibilities are legion.

In the cases we studied, police often only gained access to communications after the fact, once computers had been confiscated. This produced hours of chat logs, with many different people discussing all kinds of subjects. Sometimes the chats are purely social, but sometimes they discuss the substance of a crime – such as the best country to commit it in.

N: 'Credit card fraud is legal?'
A: 'Not illegal to host them'
N: 'Lol'
A: 'It's illegal to buy of whatever. As a hoster im not supposed to care.'
N: 'Some of my customers with illegal sites make it sho internal server error unless the referrers is google. LoL'
C: 'We have carding boards and it is perfectly legal.'
[...]
A: 'I host many cc [credit card] shops, they even appeared on krebs blog :D'
N: 'Where? Ukraine?'
A: 'HK' [Hong Kong]
C: 'Ukraine.'
N: 'I am using NL. LOL.'
– Excerpt from a chat log

Most communication in our cases was in Dutch or English and discussed criminal activities openly. From the nature of the conversations, it is apparent that those taking part felt unrestrained and safe in doing so.

A chat log found in one of the files involved regular active participants using fifteen different aliases. Their contributions indicate that they come from various different parts of the world. However, only three have ever been actually identified: from the US, the UK and the Netherlands respectively. By their own admission, they had never met in person. In another case, a blogger on the dark web has no qualms about discussing criminal matters, evidently feeling safe in that environment. Others do make efforts to protect their communications with clients, even on the dark web, although in one instance a suspect also used ordinary unencrypted e-mail to agree prices for goods he was to supply. Communications security clearly requires a level of discipline which some people are unable to maintain consistently.
Suspects often deliberately select online communications services which encrypt network traffic as standard. Many of these are 'untappable', not least because the provider is located abroad and therefore not subject to the Dutch requirement to facilitate interception. But even if they were, that would produce nothing as today's encryption technology makes it impossible to unscramble the contents of the traffic. Law enforcement agencies sometimes also need a bit of luck. During the arrest of one suspect, his Skype account happened to be open and gave police direct access to his files, aliases, contacts and chat logs and sessions. In another case, it was a

witness who handed over logs and transcripts of his chats with the prime suspect – although it is unclear why he had kept them.

Protecting data
When suspects' homes are searched, police always confiscate any data they find. But the case files reveal that these are frequently inaccessible because they are protected by strong encryption technology. In several cases, the Netherlands Forensic Institute attempted to 'crack' the encryption, but in none of those we studied did it succeed. Criminals are often very aware of the need to protect their data as effectively as possible. In one file, we read a report of a conversation with an undercover police officer, in which a suspect discusses the use of a Yubikey. This is a small USB stick that acts as a two-step authentication tool, offering very powerful data security. Suspects also swap ideas about the best way to encrypt information. The tool TrueCrypt is mentioned a number of times in this context.
In one case, the suspected group's 'IT expert' had fixed his computer to the floor using steel brackets. Next to a 'dead man's button' in his office, he also had an app on his mobile telephone to remotely switch off the power in his home. During a struggle with police as they attempted to arrest him, he managed to activate this and shut down the computer, making all the encrypted data on the system inaccessible.
Once someone has been arrested, police often need his (or her) co-operation as they can only access his secure data if he is willing to disclose his log-in details and passwords. Whether these details are forthcoming varies from person to person. At one end of the scale is the programmer who regretted his actions and co-operated fully, providing all the information requested. At the other is the suspect with the dead man's button. He refused to help in any way and invoked his right to silence. In between are those prepared to give up some details, such as the passwords for a telephone or Hotmail account, say, but not that of a confiscated laptop.

The exception
The case files describe one exception to the above rule: a suspect with enough expertise to operate undetected online, but who decided not to. In his own words, this individual had 'helped build the Internet in its current form'. According to one expert we interviewed, the NHTCU was impressed by his in-depth knowledge.
This particular person responded to a direct invitation from the NHTCU to chat about a blog he had written, and so his identity was known from the outset of the investigation. Nor did he feel any need for anonymity, since he believed that he had acted within his rights and not committed any crime. No relevant data was found on his computers, as he had a script running which irrevocably deleted his online history, passwords and other material after use. Instead, most of the evidence in this case came from a chat logs supplied by a witness, technical analyses and data found in the computer of another suspect.

3.5 The cases in Wall's typology

What does it mean that suspects use computers or the Internet to commit (organized) crime? Do they use the Internet to commit conventional crime and does the Internet give rise to new forms of organised crime? Based upon the suspects involved and the activities performed in the studied cases, we can ascertain that suspects in the Netherlands are involved in cybercrime in three ways. Firstly, there is the so-called cybercrime in a broad sense, or computer-assisted crime where existing organisations with an established track record in drug smuggling, human

trafficking and arms dealing use computers, technologies or the Internet to create *more* opportunities for their traditional crime (Wall, 2005, p. 81-82). One group, for example, sets up a website to sell drugs and weapons. Another went in search of hackers able to break into a logistics system so that containers holding drugs could enter the country unnoticed.
Secondly, we encountered groups that use the *new* opportunities that the Internet provides to commit crimes. This is called computer-enabled crime, according to Wall's categorisation of cybercrimes (Wall, 2005/15, p. 81-82). This category includes a case where after the death of a prominent figure in the Dutch underworld, relatives recruited hackers to obtain information about how his fortune was to be shared out. Another example involves a group of suspects with a background in human trafficking who redirected their efforts into skimming bankcards at cash machines across Europe.
Finally there are the new 'groups' developing specifically Internet-led criminal activities, also known as cybercrime in the narrow sense. Or, as Wall calls these entirely new types of crimes, 'computer-dependent crime' or 'true cybercrime' (Wall, 2005/15, p. 81-82). One example is developing, providing or deploying DDoS attacks, malware and ransomware. Another is stealing, selling or abusing financial data, such as credit card details. And yet another is fraud in the online retail chain. In these groups, different individuals undertake specific activities and there is no real need for them to make contact before the task is complete. Some create tools like botnets or malware, others offer them for sale on cybercrime forums, a third party buys them and yet another actually uses them to cause damage or make money. In this scenario there is no real direct collaboration between the developer of, say, ransomware and the person who distributes it. Effectively, a product is manufactured and then sold to an end user. Although there are cases in which someone who has created malware, for instance, actively seeks out people to disseminate it and makes an agreement with them to share the proceeds. Conversely, we also see individuals wishing to undertake criminal activities online go in search of accomplices able to facilitate them by hacking systems and stealing data. Moreover, the development, supply and deployment roles in cybercrime are not clearly delineated. In reality, they tend to overlap. In one case, for example, a suspect both bought malware from others and produced his own. By combining the two, he was able to teach himself what worked and what did not. Within these examples power struggles are sometimes fought out using DDoS attacks.

3.6 Collaboration and organisation

One of the questions addressed by this study concerns how suspects of cyber-OC collaborate and to what extend cyber-OC is organised.

Size and composition of criminal groups
All but one of the eleven cases we studied definitely involved some form of collaboration between suspects. The number of suspects in the other ten cases ranged from two to 49. In four instances there were two or three suspects and in another four between six and nine, whilst the two largest cases had 12 and 49 suspects respectively.[37] However, the number of persons of interest in a criminal investigation says more about the focus of that the police inquiry than it does about the scale of the cybercrimes committed. As an example, the case with just one suspect

[37] One case had one suspect, one had two, three had three, one had six, one had eight, two had nine, one had twelve and one had 49.

centred on extensive botnets with servers and millions of infected computers in several countries whereas 48 of the 49 suspects in the largest case were accused of drug trafficking offences and only one of a computer-related: recruiting hackers to facilitate the smuggling. That said, in the botnet case, although only one person has been arrested, the police and consulted experts assume that others must have been involved in maintaining and operating the networks. But they have been unable to identify anyone responsible for this.
Within the groups, these are usually some individuals who concentrate upon the ICT aspects of the operation and others who focus upon other matters. These can range from commissioning a hack to more secondary roles like receiving packages, channelling money to a safe destination, theft or smuggling drugs.
Collaborating suspects often come from different backgrounds, although some groups largely share a national or ethnic heritage: Dutch, Romanian, Ghanaian, Turkish or Russian, for example.

Organised crime: Social relationships and dynamics
One interesting question is whether or not the relationships between suspects working together on cybercrimes are similar to those in more 'traditional' or 'regular' organised crime.
According to the national Organised Crime Monitor (Kleemans et al., 1998; Kleemans et al., 2002, p. 3), social relationships such as family links and friendships are an important factor in criminal alliances. Kleemans et al. (2002, p. 3) describe these relationships as follows: *'People work with people they know, and introduce each other to others. In other words, social relationships are the cement in criminal collaboration. It is also due to such relationships that bridges are built between criminal networks in different countries.'*
Another fact revealed by the monitor is that the dynamics in the alliances investigated are highly significant. People drop out, sometimes because they are arrested, and new members are drawn in, sometimes having a snowball effect. Over time, some participants become less dependent upon others for money, knowledge or contacts, and so increasingly go their own ways – in the process often roping in other people they know. Criminal alliances are changeable and dynamic (Kleemans et al., 2002, p. 3).
In their status assessments of high-tech crime, the police point out some striking differences between organised cybercrime and its 'regular' counterpart (Bernaards et al., 2012, p. 89). For example, there is usually no offline contact between 'partners in crime', only online communication, according to this police report (Bernaards et al., 2012, p. 89). The structures are also far less hierarchical, an aspect we shall return to later.
In the files we studied, family ties, friendships and exclusively online relationships all appear. In one case, two hackers were brothers, and we also find three more instances of brothers working together. Other groups of suspects had been friends since their early schooldays and regularly visited each other's homes. There were also associates who had met through online forums and who collaborated and agreed strategies using chat software, without ever having met in person. Moreover, these different forms of relationships were intertwined. One person suspected of producing and disseminating malware worked both with someone with whom he only had online contact and with a good friend he knew from school. It is not always possible to determine from the case files exactly how online relationships and alliances originally formed, although transcripts of chat sessions, for example, do sometimes provide an insight into the nature of collaborations and the relationships between those involved.

Online contacts: known and unknown

Online collaborators often regard one another as good acquaintances, even if known only by nicknames. They may well not know where their partner in crime is located, or even in what country. Chat sessions reveal suspects pointing out how long they have been in touch, which seems to imbue a sense of trust.

Some cases, are built solely around online relationships. Suspects do not know where their accomplices come from or how old they are. There are also instances in which contacts established online – in a chatroom, say, or through a game – later lead to meetings in the real world.

In one case involving phishing and intercepting packages by delivery couriers, several of the suspects knew each other as members of the African community. Some even met through church. But it is not clear from the case file how the contacts between the phishers and the couriers first came about. In one of the cases, where hackers facilitated the trafficking of drugs, it is also uncertain how the 'drugs boys' came into contact with the 'computer boys'. These may not have been pre-existing relationships, but new ones entered into specifically in order to introduce innovation in smuggling activity by means of cybercrime. Most of the participants in a skimming conspiracy were Romanians who had known each other a long time. After several were arrested, other Romanian friends were asked to take over their tasks.

Forums

Existing relationships may engender joint criminal enterprises, but there are also cases in which people planning a crime actively go in search of accomplices with the skills needed for a particular aspect of the 'job'. These services are offered on a number of online cybercrime forums, where you can present your specialisms. There are even 'customer reviews', so that others can see how good you are at what you do. Providing a meeting place for offenders and a channel of communication between them, these forums thus serve as source of illegal activity (see also Leukfeldt, 2014). Or, as one police officer put it in an interview, *'a combination of eBay and LinkedIn in the field of cybercrime'.*

In this form, collaboration means that everyone has a distinct role, buying or selling his or her products and services online. We found several examples of this in the case files, with services or products on offer – complete with price lists – including spam services, malware, botnets and stolen bank account and credit card details. Other forums offer a platform to discuss, say, the latest hacking techniques to put people with those shared interests in touch with each other. And sometimes people are approached online with offers to undertake criminal acts for payment – for example, spreading malware by generating as much traffic as possible to advertising websites. Leukfeldt (2015) also emphasizes the crucial role of forums as meeting places, and points to the role these places could possibly play in the development (origin and growth) of cybercriminal networks. Our data shows the importance of the forums for ad hoc as well as for more long-term cooperation and for committing crimes on a local as well as on an international level.

Mutual trust and sanctions

Buying and selling services or information in this way requires a certain degree of mutual trust. This can be built up through years of online contact, and through reputation and customer reviews, but trust may also be expedited by factors like a common language, or common (ethnic or educational) background. In one of our cases, the suspects chatted in Russian street slang whilst committing crimes targeting the Netherlands. Good online feedback from fellow offenders also helps smooth the path to collaboration or orders. Another phenomenon we observed is advances or down payments being made in order to kindle trust.

Threats are part of the game, too. In a couple of our cases, suspects promised to *'send the boys round*' if a payment was not forthcoming. Online, meanwhile, a possible DDoS attack is sometimes used as a threat. Naturally, trust is an important factor in all forms of criminal association. Whether online or offline, suspects can never be quite sure they are not dealing with an undercover law enforcement officer. In the following extract from a chat session between two suspects who had been working closely together, we see how they play games around their trust in one another. Both know they are vulnerable, and try to make jokes about it. The pair has been collaborating intensively, chatting at length about obtaining and using other people's credit card details. One knows where the other is, because he has arranged for his 'partner in crime' to come to the Netherlands and found him somewhere to stay. But the other has no idea where his accomplice is located, or even in what country. The first cites their long partnership as a reason to trust him. After some time, 'A' suggests meeting up in Amsterdam.

A: 'Tomorrow we hang out. Together'
B: 'Nah. U're a cop'
A: 'I will pick u up. On new apartment. I am serious. I show you some spots'
B: 'Nah. I wont get in the car. Lol'
A: 'No not in a car'
B: 'U ll drive me to police station'
A: 'We just go and talk about some shit'
...
B: 'Who the fuck is dumb enough to reveal his identity to someone from black mar'
– Excerpt from a chat log

The forums mentioned earlier also have private sections, which can only be accessed with permission. Logically, trust again plays a major role here. In one of the cases, for instance, suspects were active in the open section of a forum but also communicated with a more select group of contacts 'behind closed doors'.

Facilitation by individuals and companies
As well as the actual suspects, the police files also reveal details of other individuals and companies which played a part in the criminal activities. These range from conscious facilitators, aware that they were abetting illegal acts, through passive facilitators – those who ask no questions or impose no conditions on a service they provide – to innocents whose contribution was entirely unwitting or unwilling. These actors can be divided into five broad categories.

1 Hosting providers – companies that rent out or manage servers. These include so-called 'bulletproof' providers. Some impose no restrictions upon what their equipment is used for. Those implicated in our cases are based in a number of different countries, including China, Russia and Ukraine;
2 Advertising firms which are used to place online ads containing concealed malware or ransomware. According to one suspect, some are aware of this but do nothing about it;
3 Front businesses – real or fake – for criminal activities, to make them look legitimate. There is a trade in so-called 'shell' companies, which can be used for activities like money laundering. In one case, a construction firm acted as cover for Romanians to travel to the Netherlands, supposedly to work in the building trade, when in reality they were here to skim bank cards. Another example is haulage businesses set up to facilitate drug smuggling;

4 People who forge or procure identity documents for suspects or, as in one case, convert cash into bitcoins. Suspects have been overheard talking about these figures amongst themselves, but in general nothing more is known about them;
5 Legitimate businesses like webshops, courier firms and telecommunications companies, which are exploited by suspects in the perpetration of their crimes – and are sometimes also victims of it. In one case, for example, products were ordered from a major online retailer using credit card details obtained through cybercrime for delivery to accomplices in the conspiracy, who then sold them on for cash. And in another case delivery couriers themselves intercepted and sold fraudulently ordered items. Legitimate firms are also used to lodge stolen funds electronically, thus avoiding the banks.

3.7 Damage of cyber-OC

A central point in the current policy on the damage and harm of organised crime is the so-called 'undermining'; meaning the intertwining of the legal and illegal structures in society.[38] In this section we discuss the damage of cyber-OC. Targets of cyber organised crime can be computers, individuals, companies and authorities. The damages caused by cyber organised crime are material as well as immaterial. In our cases a first type of damage is financial loss. In several cases hundreds of random civilians are the target of some kind of banking fraud, where their bank accounts or credit cards are used to steal their money. Because these victims are compensated by their banks, these financial losses are for the banks. Also web shops suffer from financial losses in several cases because of fraudulent credit card orders. Goods are ordered using the victims name or their credit card details. Next to direct financial losses, targeted companies have to incur costs for the investigation of frauds or improvements. Next to money, we see that sensitive information is stolen from a law firm.
A second type of damage is the unavailability and non-functioning of websites and other Internet services, caused by DDoS-attacks. This is mostly troublesome for people wanting to use these websites, but there can also be financial losses caused by the shutting down of websites, or reputational damage for the company who owns the website. Reputational damages can also be caused by the use of the National Police logo in e-mails containing ransomware.
A third type of damage that we encounter in our cases is distrust. Several kinds of cybercrimes cause banks to fear a distrust by the general public regarding online banking, e-commerce, and their own good name.

[38] *Kamerstukken II* [Dutch parliamentary papers] 2015/16, 29 911 nr. 120.

4 Criminal investigation of cyber-OC

The characteristics of cyber-OC, as described in this report, require a specific investigative approach and expertise. This influences the choices made when setting up an inquiry and selecting the methods to use. All but one of the investigations reviewed for this study were conducted by the National Police Service's High Tech Crime Unit. This is logical because, certainly with those cases we define as cybercrime in the 'narrow' sense, specialist technical knowledge is needed to understand how the suspects operate and to perform effective detective work against them. At the time of writing, regional police units did not yet possess that kind of knowledge. In this section we examine the investigative methods used and, as far as possible, the reasoning behind those choices.

4.1 How cases come to the attention of law enforcement

In none of the case files the investigation initiated as the direct result of a complaint from a single member of the public. How do cases come to the attention of law enforcement then? The cases examined for this study came to police attention in a number of ways. Large organisations like banks, Internet service providers (ISPs) and online retailers usually conduct an internal investigation when they have been the victim of a hack, spam run or cyber theft, before officially reporting the matter to the police. Of our eleven cases, however, this was done in only two. In these two cases, the target organisation first determined the scope of the incident, the number of customers affected and the financial loss suffered. They also examined the techniques used by the criminals and were able to penetrate their system or otherwise exploit it. Web shops, for example, can embed a tracking pixel in their online customer correspondence. This is unique and can thus be used to see which customer was originally sent a phishing e-mail. Banks keep an eye out for unusual transactions and, when spotted, contact the customer concerned and may block their account. They also contact victims of fraud and the holders of accounts that may be channelling funds to criminals, so-called 'money mules' – a method commonly used to collect or launder illegal gains. When the banking sector's Electronic Crimes Task Force (ECTF) decides to lodge a formal complaint with police, it also provides a supporting dossier containing the information gathered during the internal investigation. This kick-starts the official inquiry. In none of the case files we studied, however, did we find such a dossier. But we did come across some individual documents and reports originating from in-house investigators at banks or web shops.

Another trigger is information from abroad. This initiated the Dutch investigation in three of our eleven inquiries. In one case, the source was Europol. Material which had been obtained pointed to a number of Dutch suspects, prompting an invitation to the NHTCU to become part of the Joint Investigation Team. The team is an international case-specific arrangement that enables detectives from different countries to share information without having to submit formal requests for assistance.
In another case, the NHTCU was alerted after bank cards and identifiers issued by a leading Dutch bank were discovered during the execution of a search warrant abroad. An identifier is a device which generates unique security codes that online banking customers have to enter when completing transactions. Together with the bank's formal complaint, this resulted in an investigation. Meanwhile, another case was instigated by a number of reports by foreign law enforcement agencies naming

the Netherlands as the country of origin of packages containing small user quantities of drugs. These were being sent to addresses all over the world by post or parcel services. The information received led to a preliminary investigation, as provided for under Article 126gg of the Code of Criminal Procedure, in which the Public Prosecutor Service and the NHTCU monitored online marketplaces. Dealers on these sites acquire a good reputation for reliability through positive customer reviews. Therefore, the original idea was to disrupt the trade by posting fake messages under a pseudonym. It soon became apparent, however, that a number of persons active on the marketplace came from the Netherlands. It was therefore decided to shift the focus to a particular Dutch-speaking individual who was offering drugs and weapons. Although he was by no means unique, this dealer stood out for the fact that he spoke Dutch, used a Dutch nickname and was very active on the site.

'It was one choice amongst many.'
– Public prosecutor

The preliminary inquiry eventually resulted in a full-scale investigation into a group of Dutch drugs and arms dealers whose ultimate ambition was to open their own marketplace on the dark web.
One case first came to light when containers passing through a seaport failed to reach their intended destination and were reported to insurance companies as lost. At first it was assumed to be a 'simple' case of load theft, since many of the missing containers held valuable raw materials. That was why the insurers lodged formal complaints, and why police made the matter a high priority. But not far into the official investigation, investigators realised that the containers in question all had an 'extra' load of illegal drugs, which was the real reason for their disappearance.
In addition, two other investigations were sparked by tip-offs from the online community. In one case an Internet expert in Switzerland discovered malware originating from a server in the Netherlands, using tracing software he had written himself for his research into malware and botnets. The source server was operated by a legitimate Dutch hosting firm, which was unwittingly disseminating various forms of malware. The company's own subsequent investigation, in conjunction with the Swiss expert, led to a formal complaint.
Another case began after a tweet caught the attention of the NHTCU. The message referred to a report on a website that a massive DDoS attack had been successfully repelled. Wanting to know more about the background and scale of the incident, and the person behind the tweet, the tweeter was contacted by the NHTCU. Shortly afterwards, the company targeted by the attack lodged a formal complaint with the police. None of the case files we examined, was initiated as the direct result of a single complaint. However, in one case, 270 private individuals were found to have contacted the police after a major spam run had infected their computers with ransomware and rendered them unusable. This was only recognised once the police systems were searched specifically for this kind of complaint, following an internal report from the NHTCU on the use of ransomware. In this case, the name and logo of the Dutch police service were abused to make victims think it was the police blocking their computers. Open source research by the police revealed that this is a growing problem across Europe, with devices infected in the same way and the logo's of local law enforcement agencies often used as part of the deception. Victims also see onscreen messages in their own language, as the malware adjusts the language based on the IP address. It was then decided to search the Dutch police records, which is when the large number of complaints attributable to this form of ransomware was discovered. The police systems are not structured in such a way that multiple victims of the same criminal conspiracy are automatically linked; the

connection only became clear when comparable complaints were sought for in the police records. Moreover, as one interviewee pointed out, not everyone affected in this case will have lodged a complaint. Some will have been deterred from doing so because their computer was apparently blocked by "the police" as child pornography had supposedly been found on it.
Another interview with a member of the NHTCU revealed that system searches to detect complaints of possibly related cybercrimes are now conducted with some regularity. This is also done because, as mentioned during interviews, police officers at the front desk are not always sure how to proceed after such a crime has been reported.

Interestingly, in only a few case files, we found some information originating from intelligence units. Intelligence information from these units can come from the criminal community itself. It is remarkable that these squads seem to have a limited information position as it comes to cyber-OC, as one of their tasks includes identifying new crime trends and reporting on emerging crime issues (Kop & Giels 2011; Kop 2012). In the fight against traditional organised crime, intelligence from the Criminal Intelligence Unit regularly provides the starting point for an investigation. During the course of an inquiry, too, inside information can be very useful. In our interviews with experts, the topic of the police's online intelligence position was raised on several occasions. Whereas the position in relation to traditional organised crime is strong, informative and very valuable, these experts unanimously characterised the information position in the Internet as a "challenge" for the future.

4.2 Investigation instruments, methods and strategies

Investigative methods
Analysis of our selected cases reveals the use of a wide range of methods and means in the investigation of organised cybercrime – not all of them as 'high-tech' as one might imagine. Even when trying to solve the most advanced forms of computer-based crime, detectives regularly resort to logical thinking and making connections between fragments of information they have uncovered. This can help clarify what they still need to find out, and how they might go about uncovering it. Even in this domain, analytical skills are as important as the use of cutting-edge technology. In this section, we describe the methods we encountered in the case files.

High-tech methods and digital traces
Advanced 'high-tech' investigative methods are sometimes used in the investigation of cybercrime. These include SQL injections, deliberate malware infections and pixel injections. One case saw creative use of technology to prompt complaints from victims of a botnet attack, by actively warning the users about infected computers and encouraging them to report the attack. In order to reach them, the suspects' own botnet was used. Those contacted in this way were asked to complete a 'botnet victim response form' and e-mail it to the NHTCU. Forms received constituted official police complaints. It is not known how many responses this tactic generated.
Naturally, the more traditional digital traces are also taken into account: in-car GPS data, details of financial transactions, telephone and Internet usage data and so on. Even cybercriminals sometimes seem unaware of the traces they leave. In one case, for instance, data from the GPS system in a rental car was used to track deliveries of relatively large consignments of drugs and other illegal goods ordered

on the Internet. On another occasion, a car was followed electronically over a longer period, enabling events related to the crime – specifically, numerous cash withdrawals involving different 'money mules' – to be linked to its physical position.
As part of yet another investigation, transaction data pertaining to all known primary and secondary money mules was obtained from four large Dutch banks in order to trace the routing of illegally-procured funds and so reveal who their ultimate recipients were. This also allowed the banks to safeguard some of the money, because the fraud was discovered in time.
The digital traces left behind by telephone and Internet traffic are also used, of course. But we look at this topic later, under the heading 'Special investigative powers', since the interception of communications and the use of traffic data are standard, widely utilised methods in the investigation of all forms of serious and organised crime in the Netherlands.
Online detective work for of digital traces does not feature widely in the cases we analysed. The Internet is used mainly as a general source of open information, on which specific data can be found quickly. But even entering certain terms into a search engine or consulting social media can uncover useful material. For example, investigators can find out where else a particular telephone number, name or nickname appears; or who is the registered user of a domain name; or whether their suspects have accounts on Facebook or other social media. In one case, a search of this kind provided numerous photographs of the members of a criminal organisation and helped to identify money mules and other accomplices.
Finally, the Internet serves as a information source to learn more about specific aspects of a crime, such as the malware used. Useful resources in this respect include the Malware Encyclopaedia and the Microsoft Malware Protection Centre.
As mentioned earlier, though, high-tech methods are by no means the only way to investigate cybercrime. In one case, a public prosecutor told us, a deliberate decision was taken to use only offline techniques. Containers were stolen from a seaport; as well as their normal load, they contained consignments of drugs. In order to gain entry to the port to load the containers onto lorries and remove them without being challenged, the port's access control system was hacked. The investigation into the two hackers responsible for that aspect of the operation was conducted by an agency abroad. For the Dutch part of the inquiry, it was decided to stick to familiar territory and not carry out extensive digital detective work – in part because the expertise needed for that is scarce and in part because enough conventional evidence against the main suspects was available. For example, there were CCTV images of people installing keyloggers (devices that record a computer user's keystrokes and mouse movements) at the port office to facilitate the hack, as well as copious evidential material obtained from intercepted communications.

Special investigative powers
In the selected cases, extensive use was made of methods governed by the Special Investigative Powers Act. This comes as no great surprise as, for all involved forms of organised cybercrime that fall within the legal criteria for deploying those powers, the law states that this is permissible when facts or circumstances give rise to a reasonable suspicion that offences as described in Article 67, clause 1 DCCP are being prepared in an organised manner or in one likely to entail a serious violation of the rule of law. An example of the use of these special investigative powers is the use of an undercover agent acting online to make contact with a suspect to eventually meet him in person. More often, other special investigative powers are used, like interception of conversations or the use of telephone and Internet traffic data.

Telephone and Internet taps

At least one telephone tap was used in seven of the eleven cases studied. The information obtained assisted the investigative process in various ways. Tapping was instigated in order to reveal who was in contact with whom, to help understand the relationships between suspects and to identify the locations they visited. When a call is made using a tapped mobile telephone, the position of the relevant transmitter mast and other details are passed on to investigators. This enables the police to locate suspects and places they visit. Another use of telephone taps is to determine the best moment to place other forms of listening equipment. They sometimes also reveal when and where suspects are planning to meet, allowing police to deploy a surveillance team.

IP taps were also used in seven of our eleven cases – although not exactly the same seven as the telephone tap. Until 2014, these two forms of interception were registered separately. Since then, however, telephone tapping has automatically included Internet monitoring. This is due the massive increase in mobile use of the Internet on smartphones. As a result, in studying the files, it is not always possible to distinguish between information derived from intercepted Internet or telephony traffic. Internet taps are used both to eavesdrop on online communications and to monitor the behaviour of a suspect on Internet. It shows the visited website, forums and the Internet searches. In one case, messages suspects sent to one another were read by detectives thanks to an IP tap.

A server can also be tapped to reveal who is using it and to get insight into the question what traffic is passing through it. Using this technique police were able to monitor communications between those involved and discover when the principal suspect was planning to travel to Amsterdam to attend an event. From his hotel reservation, booked online, they were then able to ascertain where he would be staying. The person concerned managed an extensive system of botnets, requiring daily technical maintenance. It was considered probable that he would log in remotely in order to carry out that work and keep the system running, so police were able to take measures before his arrival in the Netherlands to eavesdrop on him whilst he was in the country.

In another case, a server tap intercepted log-in details and provided personal information about suspects. Thanks to this, police were eventually able to track down the Facebook page of the girlfriend of one of them, from which they were able to positively identify him. And in a third case, a tapped server provided functional details about other servers forming part of a larger network.

When communications or server channels are encrypted, however – a technique which is being used increasingly to protect communication – a tap will still intercept them but messages cannot be read. This makes it complicated, and often even impossible, to eavesdrop on online traffic for investigative purposes.

In the case files, we discovered numerous examples of chat sessions conducted via encrypted telecommunications services. Offenders apparently make extensive use of these services. In general, police were only able to read the conversations once a computer had been seized.

In addition, e-mails routed through foreign Internet Service Providers such as Yahoo, Google and Hotmail were found. Again, investigators only gained access to these after suspects had been arrested and their computers were examined, or after their user names and passwords were obtained. In one case, a witness gave police his archive of communications logs with a suspect.

Obtaining information from Internet Service Providers is difficult for several reasons. This has to do with the fact that not all services provided by ISPs are subject to the Data Retention Directive. Next to this, they are often based outside the Netherlands

which makes it difficult to rely on the requirements under Dutch law (Art. 13 of the Telecommunications Act) to allow duly authorised interception of data and communication on their servers. And in none of the files reviewed did we find evidence that a formal request for assistance had been submitted to a foreign ISP. The data concerned almost always came into police possession at a later date, after a suspect had been arrested. The sole exception in this respect was a request to Twitter, lodged after the NHTCU received a tip sent using its direct messaging function, to provide details of the account used in the hope that the informant might be identified. Unfortunately, this yielded no information: the account had already been closed and deleted.

Historical traffic data

The Data Retention Act (see paragraph 4.1 above) was still in force when our cases were under investigation of the police. Historical communications traffic data was requested and utilised in every single case we looked at. These requests can provide investigators with information on: what numbers were called and when, for how long and from where, as well as when the Internet was accessed and what IP addresses were used. However, content of conversations, messages or e-mails and de IP addresses of visited websites or search term entered into search engines cannot be requested based on the data retention act.

In all eleven cases, the requested traffic data were acquired and exploited by the police. Typically, traffic data is obtained when telephone numbers are encountered during an inquiry and the police want to find out to whom they are registered, who else they have called and where they have been used. In our cases, warrants pertaining to the registration of IP addresses were also obtained on several occasions. In one case, for example, secured historical data identified eleven addresses used to steal money from bank accounts with the help of malware. After suspects in the same case had been arrested, police seized a number of dongles that they were able to link to illegal online bank transfers. Moreover, it was found that 81%of all their Internet access passed through a mast close to where one of the suspects lived. In another instance, an IP address led investigators to an address across the road from a suspect's home. Indicating, that the suspect might have misused the unprotected Wi-Fi network of his neighbours.

Monitoring telecommunications and obtaining historical traffic data are not the only special investigative powers used in cybercrime investigations. Other online and offline methods include pseudo purchases, infiltration, systematic observation and remote monitoring of communications ('bugging'). In the Netherlands, however, infiltration and bugging a suspect's home or car are regarded as particularly intrusive techniques that severely impinge upon a suspect's privacy – far more so than eavesdropping on their telephone calls. But research has shown that different countries have very different attitudes in this respect (Odinot, De Jong, Van der Leij, De Poot & Van Straalen, 2012). In England and Wales, for example, infiltration is regarded as less intrusive than telephone tapping. By contrast, Dutch investigators must demonstrate a sufficiently serious breach of law before they are authorised to deploy such methods. As a result, the number of infiltration and bugging operations conducted in the Netherlands is very limited (Kruisbergen, De Jong, & Kouwenberg, 2010, p. 136-37). This makes it all the more striking that we find both in inquiries we examined.

One or more suspects were systematically observed in four of our cases, and in one police made pseudo purchases in the form of orders placed on a website on the dark

web. In addition, one investigation involved the use of an online and offline undercover agent and in another case a listening device was installed in a car.
In the former, a Dutch vendor was offering weapons and drugs for sale in an online marketplace. The infiltration began with contact through the site's discussion forum. A pseudo purchase was also made. The use of nicknames is standard practice on the Internet, and criminals generally utilise false or untraceable IP addresses. This makes them difficult, if not impossible, to identify. The police were completely in the dark as to who was behind this offence, and so needed any clue they could find. Uncovering the identities of the members of a criminal organisation responsible for a very serious crime was deemed sufficient justification for the deployment of, by Dutch standards, extreme methods in this case. It was hoped that the pseudo purchase would provide the necessary clues. Upon receipt, the ordered goods were painstakingly examined for any evidence that might lead back to the sender. Eventually this was found. The online contact also bore fruit, resulting in a meeting (offline) between the undercover agent and the suspect. He was then followed back to his home address and there systematically observed, which led to the identification of other members of his criminal organisation.
In another case, a car was bugged in the hope of identifying the key figure in an illegal online marketplace. But this individual consistently used only a nickname, so the exercise proved unsuccessful.

Interrogations and interviews
From the files it was learned that during most criminal investigations several people and suspects were interviewed or interrogated. The suspects were mostly interrogated after their arrest and these conversations are part of the studied cases. In some cases, money mules or family members of suspects were also asked questions.
The police hope to get information from these people about the acts and suspects of the criminal organization. The police try to get an impression of the individuals of the criminal organization, how the suspects are related and how they know each other. Sometimes a witness contacts the police on their own initiative. One female for instance, testified that a suspect had used the bank account of their son to launder money. In another case, an acquaintance of the main suspect contacted the police and provided logs and content of communication he and the suspect had in the past.
Most suspects themselves however, are not very willing to share information. If suspects are willing to talk about their activities this is often only during their first interview. After they had consulted their lawyer, in many cases they refuse any further collaboration and invoke their right to remain silent. For this reason interrogations are not very successful in getting information about login details to give the police access to encrypted files. Sometimes suspects do cooperate and give a particular password. For instance, they provide a code to their telephone but not to their Gmail and Hushmail account. Or someone can be willing to give the entry code of their laptop but not to specific encrypted files. This can be very frustrating. Getting enough evidence for a conviction is extremely difficult in such cases.
Sometimes suspects give a reason for their refusal to talk. One suspect, the administrator and head figure in the criminal organization, said he was too scared to testify. He was threatened; '*Silence is gold, talking is dead*'.
On a rare occasion some suspects testify about how they were supported in their activities or modus operandi.

'With his money, I bought programs that we might need. I liked that, because I didn't have the money.'
– Excerpt from a forensic interview

One suspect testified that he was not guilty. During his testimony he gave a detailed technical explanation why he thought that his actions were not the cause for the criminal acts. This person provided specific instructions on how to deduce and interpret some computer logs.

Tracing money mules
In interviews with experts we were informed that tracing the money mules had a substantial role in police investigations on cybercrime cases. In addition, during the research, we found several examples of cybercriminals using money mules to launder money and to hide the identity of the suspects. The money mule receives a fee for his or her services, but may not always be aware of the illegal nature of the activity. Often, these people can be described as vulnerable, living in difficult social circumstances or having addiction problems. After being convicted or fined as a money mule they are placed on a black list which makes it difficult for them to get a mortgage, loan or other service from a bank for a long time. Preventing them from becoming a money mule by providing adequate information might be worthwhile (see also Leukfeldt, 2014). If the general public knows that lending your bank account for a small amount of money is a crime, it makes it more difficult for cybercriminals to cash stolen money. Efforts to inform people about this matter are taken by Dutch banks.[39]

Focus on facilitators in cybercrime investigations
In the Netherlands, in the fight against traditional organised crime, there is always special interest in and attention paid to the facilitators of crime, such as car rental companies or transport businesses. In our studied cases on cyber-OC, the police also revealed facilitating individuals and companies that played an important role in the criminal activities. These facilitators range from people or companies who know their involvement is abetting illegal acts, to facilitators who are unaware of their role and whose contribution was entirely unwitting or unwilling.
In the cases, we found examples of facilitators for money laundering: people who convert cash into bitcoins; and legitimate businesses such as webshops, courier firms and telecommunications companies, which are exploited by suspects in the perpetration of their crimes – and are sometimes also victims of it. These facilitators in the digital world are not the same parties as we know from offline organised crime cases and they offer new possibilities for law enforcement and prevention in the field of cybercrime. It is worth investing in the involvement of these parties in the prevention and detection of cybercrime. An interesting example in this light is the ITOM project, in which these new facilitators are informed and involved (Eurojust, 2014).

Criminal intelligence on the Internet
The capacity and resources of the police are, of course, limited. To get to grips with traditional organised crime groups the Dutch police have a special unit, the Criminal Intelligence Unit (CIU). This unit provides information about or from within traditional organised crime groups and can be used as a starting point or might be helpful during an investigation. People from the CIU may be familiar with some people in a criminal group and provide information about criminal activities. Neither the CIU nor

[39] See for instance: www.veiligbankieren.nl/fraude/geldezels/.

the High-Tech Crime Unit has a comparable information position yet in the Internet community. During our research, several interviewees think that holding a good information position on the Internet would be a valuable development in the fight against cybercrime. Several interviewees mention this as a goal for the future because developing a strong information position would make it possible to focus on important players and facilitators in the field of cybercrime, as these specialists play an important role in the phenomenon Crime-as-a-Service, and often act on an international scale. Identifying these players in the field of cybercrime might work to disrupt and counter cybercrime on a global level.

4.3 Special expertise

The NHTCU is a dedicated police squad with a well-educated workforce made up of both general investigators and IT specialists in subjects it regularly has to deal with, such as malware. When the team lacks know-how, it seeks the assistance of outside experts. This occurred in one of the cases we studied, where the suspect himself was very much a specialist in technically-complex matters which played a role in the crime: building and operating botnets. This made it particularly difficult to conduct an investigation without him noticing. External expertise was therefore called in, to help the NHTCU dismantle the complex system of botnets and safeguard evidence. The company contracted for this purpose had already studied the system itself, possessed up-to-date information about the botnets used and was familiar with the network infrastructure. All the actions recommended by this firm were carried out and recorded by the NHTCU.

4.4 Identifying suspects

Many names and nicknames appear in the case files we studied, and our expert interviewees admitted that tracking down an Internet user's true identity can be a complex puzzle. It is relatively easy to remain anonymous online, using readily available and often free software. Proxy servers and virtual private networks (VPNs) are mentioned several times in the files as means used to conceal identities. These methods channel traffic through an intermediate server (the proxy), adopting its IP address and concealing the user's own IP address and location. Anonymization software is mentioned on a number of occasions as a way of e-mailing, chatting, maintaining contacts in a chat room and exchanging information about criminal activities without disclosing who you are. This kind of software is also needed to access servers on the dark web, where we find sites offering drugs, weapons, contract killers and so on. The dark web is a part of the Internet not 'visible' to search engines like Google.

Identifying suspects proved a huge challenge for investigators in quite a few of our cases. But names were eventually put to the principal suspects in most. Had they not been, the police investigation would probably have been wound down or shelved. But even in some cases that have been cleared up, some outstanding suspects are still unidentified: people known only by their nicknames. Smart technology and clever tricks have made it simply impossible for police to find out who they really are. For example, one individual managed to keep his or her identity secret by using Tor on a hacked server. That server acted as a proxy, frustrating all efforts to trace the user's real IP address.

Various experts cite suspect identification as one of the main stumbling blocks in the fight against cybercrime. They describe it as a complex puzzle, which police can only solve by combining numerous scraps of information from all kinds of different sources. Sometimes that solution might come from a telephone number unearthed during the inquiry, for example, from a nickname that appears in different places or by linking an e-mail address to someone close to the main suspect. In one case, a breakthrough came from trawling through countless chat sessions between numerous individuals, linking a nickname to a birthday, Facebook posts, e-mail addresses and the name of a tiny village somewhere far away. This despite the suspects using Tor and e-mailing each other through an anonymous mailbox and further complicating the investigation by using nicknames: Kwik, Kwek, Kwak, Kwiek and Pietje. On this particular occasion, moreover, investigators were fortunate in that an anonymous informant had provided them with the content of the TOR mailbox the suspects were using. Even so, the nicknames made it especially hard to discern who was responsible for particular actions and how the criminal group divided up the roles in its criminal conspiracy – information which was essential to understanding how the organisation worked and to building a case against the individual suspects.
The files reveal that even some of those involved did not know who was using a particular nickname. In one series of chat sessions, for example, we see someone trying to play two other people off against each other, despite the fact that they knew each other well in the 'real world'. Transcripts of their interviews show no indication that these latter suspects were aware that their close known associate was the person behind a given nickname. This even though one did, under interrogation, disclose the real identity of someone else using another nickname.
In another case, a suspect was unaware that his partner in crime was in fact a juvenile living in a different country. They had never met in person.
In short, the search for the true identities of cybercriminals can be complicated and time-consuming, and is not always successful.

> *'Jupiter has made what Whannahave and Bob Marley asked him to, but apparently it doesn't work properly.'*
> – Excerpt from a chat session

4.5 International cooperation

Because the Internet knows no physical or geographical borders and cybercrime, too, is often international in nature, it comes as no surprise that seven of the cases we studied have a substantial transnational component.
One stands out not so much for the extent of cross-border co-operation in its investigation as for the international character of the crime itself: a complex case in which botnets were controlled from dozens of servers rented from a Dutch hosting company. Millions of computers all over the world were infected with malware which made them part of these systems. At least one suspect who was in sight of the police, designed and set up the botnets, and managed them with a view to renting them out for illegal activities. A tip-off to the hosting firm from a blogger-investigator in Switzerland initiated the criminal inquiry, which was conducted entirely by Dutch police. After a technically complex and legally challenging investigation, they managed to identify a suspect and arrest him during a visit to the Netherlands. The person concerned did not come from or live in this country, and after his arrest he was extradited to his home nation to face trial there.
In three instances, cooperation with law enforcement agencies abroad helped to track down or capture a criminal group. On one occasion, German police took over

from their Dutch colleagues after a suspect, they were physically tailing, crossed the border. In other cases, servers abroad were secured or sealed at request of the Dutch authorities. Furthermore, an arrest was made in another country in response to information supplied from the Netherlands. It was only at that point that it was discovered that the suspect was in a fact a juvenile, something even his Dutch 'partner-in-crime' apparently did not know. In all of these cases, the bulk of the investigative work was done by the Dutch police and the contributions from foreign agencies followed formal requests for assistance when international help was deemed necessary. Such requests are also used to obtain information from private entities in other countries, such as Internet Service Providers, telecommunications providers or hosting firms.

Our expert interviews revealed that obtaining assistance in this way is not always a smooth process. One public prosecutor told us that it can take up to a year to receive a response from abroad either because of procedures or because of (probable) misunderstanding at foreign corporations, who are supposed to have information.

Requests for IP address registration data or the usage records of foreign telephone numbers, for example, often pass through a long procedural chain and so take a long time – far too long, in some cases – to produce results. Other interviewees also expressed their frustration at these delays. Some of the information regularly asked for, such as telephone or Internet traffic data, is 'perishable': it is only kept for a limited period, and then deleted. If a formal request for assistance takes too long to process, there is a good chance that the material no longer exists, which can slow down or even stall an investigation. As one person told us, *'Internet activity can be fast and fleeting, and so demands a rapid response'.* In other words, formal requests for assistance are dealt with at a pace incompatible with the speed of the Internet. Having to wait for information reduces the likelihood that a case will be completed successfully. Unfortunately, moreover, some requests get no response whatsoever. We found one such instance in a case where members of the public had their computers infected with ransomware.

> *'For requests for legal assistance to be dealt with promptly, you are dependent on whether or not it is seen as a matter of priority to the country in question.'*
> – Public prosecutor

Two of the cases we studied were handled by a so-called Joint Investigation Team (JIT). An international police body set up to tackle specific cross-border criminal conspiracies, this considerably simplifies the exchange of information and lines of communication between detectives in the participating countries. Its costs are also shared between the states involved. A number of the police officers we interviewed stated that the one great benefit of a JIT is that it eliminates the need to submit formal requests for assistance from abroad. Europol plays a major role in these arrangements by facilitating the collaborations between countries. It gathers together the evidence collected by the different teams and makes it available to all participants at a central point within the secure Europol system. This material is only provided in its original language and nothing is translated. Items such as chat sessions in Russian pose a real challenge for Dutch investigators, and an official translator is only called once a Dutch version is needed for evidential purposes. Until then, police are reliant upon colleagues with some knowledge of the language and tools like Google Translate. Our interviewees do not categorise this as an insurmountable problem, though.

As well as managing evidence, Europol also analyses the data collected. The experts interviewed for this study spoke very highly of the quality of this work and the Euro-

pol analysts responsible for it. They also praised the fact that combining all the evidence from the different countries keeps lines short, and that no time is lost processing requests for assistance. In one of the cases we looked at, dealt with by a JIT, a weekly conference call that was held so that the investigators in all the participating countries could share information and ideas. They also met in person on a number of occasions, again facilitated by Europol.
Such arrangements lower barriers, making it easier to simply pick up the telephone to consult with a counterpart abroad. Detectives are not hindered by legal obstacles during these conversations, and they do not need approval or authorisation from 'the powers that be'. Overall, our interviewees were very positive about working in JITs: *'All Europe one big JIT!'*. In particular, they believe that lines of communication should always be kept as short and direct as possible when investigating cyber suspects.

Exchanging information with foreign law enforcement partners is sometimes complicated when there are no common interests or priorities. In one of the cases for example the international collaboration was not as desired. Ransomware was being distributed in a number of European countries. Before their computer was blocked, victims saw a message in their own language claiming to be from local police, and under their logo, stating that child pornography had been found on the device and it could be unblocked upon payment of a 'fine', using vouchers. The 'localisation' was based upon the computer's IP address. Investigators in the Netherlands identified a foreign suspect who had already been arrested in his own country for money laundering. For the foreign police, that fact removed any direct need to assist the Dutch inquiry. Because this case which had claimed victims across Europe, both Europol and Eurojust were enlisted in an attempt to instigate international co-operation. Numerous documents were translated to and from English, at substantial cost in terms of time as well as money. According to the Public prosecutor concerned, the Dutch Public Prosecutor Service also put in considerable effort by preparing 'ready-to-use' information packs to help kick-start criminal investigations in other countries. These even included codes enabling certain vouchers to be tracked on the Internet. But there was no response from the countries contacted. This probably had to do with the fact that it was not a priority for the law enforcement agencies abroad. When a country has some national interest in an investigation, co-operation tends to be smoother. But the huge scale of cybercrime on the one hand and their own limited expertise and capacity on the other mean that agencies are forced to make choices. That was why this case was not taken up at the European level, even though it had affected numerous victims and several potential suspects had been identified. However, the Dutch investigation did result in three arrests. Because the inquiry was still on going at the time we studied the file, we do not know how it subsequently unfolded.

> *'Child pornography and drugs are generally high on the agenda. At any rate, higher than solving extortion by means of vouchers.'*
> – Public prosecutor

4.6 Detection and confiscation of assets

The authorities in the Netherlands have been able to confiscate the proceeds of crime – or, in Dutch legal terminology 'illegally-acquired benefit' – since 1983. Under the motto 'hit them where it hurts most' (Nelen, 2004), this approach is intended to prevent crime as well as punish it and has become a central tool of law

enforcement. Powers in this area were extended in 1993 by what is popularly known as the 'Pluck 'Em' law, which enables the recovery of proceeds from crimes that have not been prosecuted (Kruisbergen, Van de Bunt & Kleemans, 2012, p. 229).

In practice, however, tracing criminal incomes is not an easy business. Moreover, policy and practice in this field diverge somewhat. A 1998 study by the Research and Documentation Centre of the Ministry of Justice concluded that 'by no means has deprival-driven thinking yet penetrated all levels of the police organisation' (Nelen & Sabee, 1998: 112-113). In 2012 the Inspectorate of Public Order and Security observed that financial investigation had still not been sufficiently integrated into the work of the police (Inspectie Openbare Orde en Veiligheid, 2012, p. 10). This is reflected in the files we studied. In only one case there was any form of financial investigation – in this instance into money mules. Inquiries focused on tracking the route stolen money had taken, which revealed a number of different scenarios. Firstly, some of the money was safeguarded because the bank spotted the fraud as it was happening and was able block accounts or reverse transfers in time. Otherwise, it was either withdrawn immediately after the fraudulent transaction or first transferred to a mule's account, and then perhaps to a second-line mule, before being converted into cash. According to the file, almost € 350,000 was made safe. This reduced the banks' losses from a potential € 600,000 or so to an actual € 270,000.

There are large differences between our cases in terms of the amount of money made from the criminal activities. Some involve huge sums, generated by distributing malware, renting out botnets or skimming bankcards. Proceeds range from more than a million euros in one case, and in another case a similar amount converted from dollars into e-currency over the course of a year, to no discernible revenue in cash or virtual money in some other cases. In these instances, the files give no indication as to how much the suspects might have made. Once converted into electronic currencies, the proceeds effectively pass out of sight. This probably explains why a financial crime investigation was initiated in only one of the cases we studied.
From the files, it is not always clear whether the proceeds of the crimes have been recovered. In some cases, the amount taken has been calculated, but little or no money is found when suspects are arrested. Of course, not finding a criminal income does not mean that no money has been made with the committed offence. In one of the cases, for example, the file reports that the prime suspect deposited US$700,000 into a WebMoney account in 2010. This was discovered following an international request for assistance, yet neither the origin of the money is known, nor what it was being used for. In open sources, there is speculation that the person concerned was making about € 100,000 a month from his criminal activities[40], but the file does not mention of large amounts of cash, assets or luxury goods being confiscated. In this specific case, that may be because the suspect was not Dutch and was eventually prosecuted in his home country. In addition, the police investigation focused upon finding evidence of the crime itself rather than its proceeds. On other occasions, police do calculate the likely revenue from criminal activities and yet recover only a fraction of that amount when they come to make arrests. In one case, the suspects were estimated to have collected more than 1 million euros from cash withdrawals around the world after skimming bank cards, but the main suspect

[40] www.bbc.com/news/technology-18189987; www.huffingtonpost.com/2012/05/24/georgy-avanesov-found-guilty_n_1543687.html; http://krebsonsecurity.com/2010/10/bredolab-mastermind-was-key-spamit-com-affiliate/, retrieved May 2016.

was in possession of just over € 200,000 when he was brought in by police. It is not known what happened to the rest of the money. In this case, recovery proceedings were initiated against four suspects, based on an estimate of their respective shares of the profits. Although they refused to comment on this matter in their police interviews, intercepted conversations indicated that they had indeed agreed a share-out. According to those communications, they worked with at least three unidentified foreign partners, who took on the technical aspects of the fraud in return for a portion of the profits.

A: 'If we divide our profit like this: 40% yours, 40% mine, 10% coders 10% traffer…'
B: 'Yeah, it's good.'
A: 'OK.'

D: 'We understand each other? So later no problems?'
F: 'Yes!!!!!))'
D: '35% you, 15% [name of suspect], 50% i share with my man and people. OK.'
- Excerpt from a chat log

Other intercepts reveal that this group regularly swindled its partners. By claiming that successful transactions had actually failed, for example, or that someone else had cleaned out a bank account. Exactly how much was made from these activities is not entirely clear, but the proceeds per suspect calculated for the recovery proceedings range between € 45,000 and € 245,000.
In only one file the stolen amount is mentioned explicitly. Fraudulent transactions at a Dutch bank, followed by cash withdrawals by money mules, netted a total of approximately € 500,000.
Police searches sometimes yield quantities of cash or expensive purchases. Suspects are often found to keep large sums of money at home, in some cases well-hidden. In one case, for example, a bag of money was discovered in a vat of rice. Searches also turned up the key to a safety deposit box containing more than € 50,000 in cash. According to the suspect's mother, the box was registered in the name of her young daughter – the suspect's sister – and she, the mother, was the authorised key holder. Another suspect in the same case, lived in Belgium, where he had more than a million euros in cash in his home. He also had substantial assets in the country of his birth. It is not known whether the Belgian authorities confiscated his money and property.
In another case, one person's proceeds from the crime were calculated to be € 30,000. Two others were also involved, but it is not known how much they made.
High-end electronics and other luxury goods are also seized. In one of the cases, suspects' homes were found to be piled high with boxes of new clothing and expensive shoes. Most of these had been ordered from webshops under false identities and were either to be resold or retained for personal use. Discoveries of expensive electronics – Apple products, laptops, TV sets, Blu-ray players and so on – feature in several other cases. Other confiscations include high-end cars, such as a Mercedes-Benz and a BMW. However, in only one instance are bitcoins known to have been seized. Other files mention the use of such cryptocurrency, but do not say whether any was recovered from arrested suspects.

Money management and laundering
Money is an important motive for the suspects, but what they earn has to be laundered first to make it appear legitimate before they can use it. The case files contain several examples of laundering practices. In one instance, some of the proceeds of

skimming were passed through a casino. Over four nights, a total of € 100,000 was legitimised in this way. Other methods used by the same group were buying electronic money and vouchers, transferring funds to the accounts of money mules and then withdrawing them in cash and ordering goods from webshops for resale or their own use. In another case, money was channelled to safety through a network of shell companies.
The files also indicate widespread criminal use of a variety of digital currencies and services. Interestingly, most of the information about these was gleaned from telephone and Internet taps. In one case, for example, e-mail intercepts allow us to track an exchange of money into a virtual currency through Western Union. An online chat sessions from another case reveal suspects logging into online banking and then converting funds through various electronic payment systems to pay overseas contacts for services rendered.
Communication intercepts show that PayPal, MoneyGram, Western Union, FBTC Exchange, WebMoney, Bitonic and xmlgold.eu are amongst services used to transfer money. Prepaid cards and vouchers are also widely used, as is so-called underground banking. In one case, cash was deposited with an underground bank and could be retrieved by presenting half of a bank note torn into two. The suspect and the bank each retained one half, and a match between them was deemed proof of entitlement to the money.

In two cases, suspects arranged to meet face-to-face in a public place like a motorway service area to exchange cash for bitcoins, or vice versa.
Bitcoins make an appearance in four of our case files. Buying them and then re-exchanging them for euros, a process known as cashing out, is regarded as enough to break the tell-tale paper trail needed to track laundering. Bitcoins are not anonymous in themselves, but can be made anonymous by using a so-called mixing service. This conceals the link between the bitcoin's identifying number and any particular individual. Exchanging bitcoins for cash also makes it hard to connect a person to a sum of money. The suspicion that such techniques are used for laundering purposes is raised by the fact that some payments originate abroad even though there are reliable domestic Dutch alternatives, which generally offer a better rate of exchange than foreign trading platforms. In all four cases, however, the bitcoins found represented only a relatively small proportion of the overall haul, compared with the amount of cash or goods recovered.
In one case, a PC used to mine bitcoins was seized. But the file does not reveal whether any actual bitcoins or other funds were found. A 'miner' is a powerful computer used to validate transactions on the bitcoin network and record them in the blockchain. The miner retains a fee for this service paid in bitcoins. A large amount of other property at two addresses was also seized as part of this investigation, including tablets, computers, hard disks, mobile telephones and a car.
In two cases, police made inquiries into the earnings and assets of specific suspects. Both entailed formal requests for assistance to Lithuania to examine WebMoney accounts. Founded in Russia in 1998 but now used throughout the world, WebMoney is an online payment method which uses a so-called e-wallet for the transfer and receipt of funds. What makes it unique is that transactions are conducted in its own WM units (WMZ) and then converted into the user's chosen form. As well as conventional currencies like US dollars and euros, options also include gold and bitcoins. However, both requests in these cases concerned the contents of e-wallets pegged to the US dollar. It was suspected that they were being used to launder the proceeds of crime and so conceal an illegal income. In one instance, a person had received a one-off payment of almost US$700,000. The source was unknown, and there were no other transactions on the account. In the other, someone had moved

thousands of euros worth of his WM units through his e-wallet over a short period, despite having a negligible legal income at the time. In all, almost 156,000 WMZ were deposited and then withdrawn in just a month. The incoming transactions consisted mainly of transfers from financial service providers, where the suspect had exchanged bitcoins for WMZ. The outgoing ones included payments to other financial service providers to buy virtual currencies like Paymer, PerfectMoney and bitcoins, but also to providers of technical solutions like proxy servers, to suppliers of the personal details of potential victims and to website hosting and maintenance services. The suspicion was that WebMoney was being used to launder money, to distribute the proceeds of crime, to conceal assets and to pay for criminal services.

The case files reveal that not all the high-earning central figures in the extensive networks under investigation have been identified. They include the owner of a marketplace for drugs, weapons and other illegal goods on the dark web. Despite focusing their efforts upon this individual, police have been unable to identify who the person is. According to one suspect in the case, the site in question had a monthly turnover of US$9 million in the last three months of its existence. Payments were made using a wallet system: the buyer paid into the wallet when they placed an order and the seller was paid from it once the goods had been received, with the owner of the site retaining a percentage. Whilst the owner remains at large, the site's administrator has been arrested. Although he was also paid a percentage of revenue for his work, he was not found to be in possession of large sums of money.
In one of the larger cases we examined, the individual at the heart of the network was identified. He turned out to be a well-known underworld figure, who had already amassed a large criminal fortune. Unfortunately, he fled to his country of origin before he could be arrested and is now beyond the reach of the Dutch authorities. However, investigators did find 1.3 million euros cash at his former home.

Convictions
At the time of writing (November 2016) ten of the eleven studied cases have been brought before the court. Of these cases most suspects were convicted for a prison sentence, community service or a fine. In one case the suspects appealed, which led to acquittal for two suspects. An interesting fact is that several cases involve foreign suspects, which have also been convicted in the Netherlands. Finally, there is one case of which the status is currently unknown.

5 Conclusions and discussion

Our research explored how criminal groups involved in criminal activities on, via and against the Internet operate by focusing on their modus operandi, the organisational structures of the crime groups, and the profiles of the offenders involved in these groups. We also addressed the challenges and obstacles law enforcement agencies encounter when tackling these forms of cybercrime.
Our findings are based on analyses of police files of eleven selected criminal investigations into organised cybercrime. The studied cases focused on different crime acts, which can generally be divided into four broad crime types, namely: 1) cases related to bank fraud, fraud involving payment systems and other kinds of fraud and money laundering; 2) cases related to the production, trade and transportation of illicit goods and services (online sale of drugs or DDos attacks, Botnet rental, hacking to facilitate smuggling); 3) cases of extortion to gain money or power (ransomware and DDos attacks); 4) cases of data theft (through hacking).

Among the case files we analysed, we saw a variety of crimes and crime groups. On the one hand, traditional crime groups engaging in cybercrime and using cyber expertise, common knowledge about the use of Internet or specific tools to perform their criminal activities more efficiently or in a more sophisticated way. On the other hand, there are new groups developing specific cyber-related criminal activities or becoming active in sophisticated forms of illicit trade via the Internet. For these different crimes and crime groups it holds that the activities have more or fewer 'physical crime components', and that the cybercrime touches the physical world in different ways. The new emerging issues and challenges related to cyber-OC we encountered in this study mainly originate from activities occurring in the virtual world.
In the eleven analysed cases 107 suspects were identified. Of these suspects at least 39 played a role in ICT-oriented activities. As the Internet entails many shielding opportunities, identifying suspects is one of the major challenges law enforcement agencies have to face. The number of identified suspects per case ranges from 2 to more than 40. The number of identified suspects depends on both the nature of the case and on the perspective of the law enforcement authority responsible for the case.
The age of the identified suspects varies highly, even within individual cases and within individual crime activities. In some cases the cyber offenders were remarkably young. Cyber organised crime seems to attract younger offenders more than traditional forms of organised crime do. In traditional forms of organised crime, young offenders are quite exceptional.[41] In the studied cases suspects come into view which we usually do not see in traditional organized crime cases, namely: young offenders; suspects with an IT background; suspects who are ill or disabled and who barely leave their house. This leads to the finding that features of suspects that may be important in the offline world, are less important in the online world. While in the offline world, when people interact and collaborate with others they go upon features like age, physical health, and social behavior, the importance of these features seems to be different within online cooperation. Because of this, partnerships can occur that are less obvious in the offline world.

[41] See for instance Kleemans & De Poot, 2008; Van Koppen, De Poot, Kleemans & Nieuwbeerta, 2010.

Involvement of organised crime groups in cyber crime
Based on the analysed cases, we see different kinds of involvement of organised crime in cybercrime. Firstly, we see (groups of) suspects that utilise the Internet to commit traditional organised crimes. These (groups of) suspects commit conventional crimes, such as drug smuggling, and use the Internet to get access to information, or to steal certain information. These suspects hire a hacker to do so, for example. This way of using computers offers *more* opportunities to commit traditional crime and falls under Wall's category of 'computer-assisted crime' (Wall, 2005/15).
Secondly, there are suspects that utilise the *new opportunities* that the Internet provides to commit traditional crimes. Within this category we see conventional crimes that are now committed online. Here we see for example new forms of trade via online marketplaces where drugs and weapons are sold online. The Internet provides an online market that offers a broader clientele on a global level. Another example is suspects who manipulate software to enable new ways of skimming. These crimes are not necessarily new, but are evolving in line with the new opportunities online and therefore becoming more widespread. According to Wall this is known as 'computer-enabled crime' (Wall, 2005/15).
Thirdly, we saw organised crime groups committing entirely new crimes that do not exist offline. The Internet makes it possible to commit new online crimes. Wall calls these entirely new crimes, like blocking someone's computer or performing a DDoS attack, computer-dependent crime or 'true cybercrime' (Wall, 2005/15).
Within cooperating groups of suspects, there are usually some individuals who concentrate upon the online, computer or ICT-related aspects of the operation and other people who focus upon other offline, more traditional matters. Individuals often have their own expertise. This can range from commissioning a hack or writing a script to more secondary roles such as delivering or receiving packages, channeling money to a safe destination, theft or smuggling drugs.

Using the Internet to commit traditional organised crime
In our data we did find groups who used the Internet to commit traditional crime. They were active in importing and selling drugs as well as in stealing documents and selling weapons. One, for example, set up a website to sell drugs and weapons. Another called on hackers able to break into a logistics system so that containers holding drugs could enter the country unnoticed. Also in this category are the relatives of a prominent figure in the criminal world who, after his death, recruited hackers to obtain information about how his fortune was to be shared out. In addition, there are suspects with a background in human trafficking who redirected their efforts to skimming bank cards at cash machines across Europe. One particular group diverted their activities from traditional crime and became active in skimming on a large scale.
Traditional groups also use the Internet for their communication. The fact that online communication services use encryption appears to be an important motivation to start using these new methods for their 'internal' communication. It avoids detection and/or interception by the police. These examples show that the Internet offers traditional crime groups both *more* and *new* opportunities to commit traditional crime (Wall, 2005/15).

Windows of opportunity
This study has shown that the Internet provides for new business ideas and new targets. The role of the Internet is stressed in order to see to how traditional crimes and organised crime are evolving into new forms of organised crime. It goes without saying that the Internet has also allowed organised crime groups to commit new

crimes (i.e. DDoS attacks, malware, ransomware and hacking) that would not have been possible otherwise. This means that ICT functions as a tool to increase the efficiency and economic gain of crimes. The cases in our study show that the Internet allows organised crime groups to come together and to work together in new ways. This is exemplified by the collaboration between people with special expertise and important contacts. In the course of this study it has become apparent that not all cybercriminals have the necessary technical skills, but they manage to 'buy' these skills or even complete malware packages to commit various cybercrimes. In one case we saw a good example of such a joint operation of suspects. They used the Internet to execute payment fraud on a higher level by violating both the users' computers and smartphones. The Internet makes it a lot easier to accomplish crimes, as offenders are able to build online relationships and collaborate without physically meeting each other. The use of forums and other communication services allows offenders to collaborate across borders. Anonymity plays a crucial role here, as there is a relatively low risk for offenders. The Internet provides for a faster global impact and, in effect, this is what characterises crime in cyberspace.
Regarding the new windows of opportunity for identifying and approaching new targets of organised crime groups, the Internet has certainly made it possible to reach different targets more easily. We can make a distinction between the types of targets, namely the victims and the customers of the offenders, in other words, people found by the offenders and those who contact the offenders. For the first type, it is important to notice the difference between what Wall (2014) calls 'technical victimisation' and actual harm. 'Technical victimisation' refers to the receipt of a phishing mail, which most people will ignore. However, this touches on the new ways of identifying and approaching new targets. When compared to traditional crimes, the Internet provides simpler new ways to reach victims. Through phishing attacks, hacked databases and different kinds of malware it is possible to reach victims without picking out specific individual targets. These targets become victims because their computer or personal information is in some way compromised. Also the damage is different, as it is possible to steal a little money from thousands of people, amounting to the same (or more) as from traditional crimes.
When it comes to the second type of targets – the customers – these are people who approach the offenders and buy goods and services from them. These include narcotics and weapons via the dark web, but also Crime-as-a-Service, which in fact also lowers the entry barriers to cybercrime for offenders. In addition, this may be seen as a new business idea, where the offender solely offers services. As revealed in this study, the Internet has allowed traditional localised drug crimes to turn into global crimes with customers all over the world. In addition, exploit kits and other tools are bought online to commit different crimes. Considering the new marketing channels, this has lead to new opportunities to get in touch with targets. However, without customers the system does not work. In the end, one might say the globalisation of crimes is not a new opportunity but rather an evolution of traditional crimes.

Structural changes in organised crime
One of the general findings based on the studied cases is that the Internet makes it much easier to come into contact with co-offenders with specific skills, to explore markets of producers, sellers and buyers of illicit trades, and to encounter (large groups of) victims. This definitely reduces the complexity of organising crimes that consist of multiple activities scattered temporally and geographically and that require collaboration with diverse co-offenders (Kleemans & De Poot, 2008; Van Koppen et. al., 2010). The Internet has changed both the routine activities of the offenders and the social opportunity structure needed to commit these crimes. In

theory, offenders can stay behind their computers to coordinate activities, collaborate with co-offenders and commit their crimes. In that sense, crimes that require coordinated activities executed by different subjects seem to become less complex and more accessible to larger groups of people. This leads, apart from changes in the modus operandi and changes in the target groups, which have already been discussed, to 1) new players in the field, 2) new forms of collaboration and 3) new economic structures.
The studied cases show new players in the field that were not involved in organised crime before. Most notable are the new groups of facilitators, consisting on the one hand of people who are technically skilled, and on the other hand of online advertising firms, webshops and telecommunication companies. In the studied case files, we encountered new kinds of front businesses, used for the transportation of money and goods, and new legitimate businesses such as webshops and courier firms that are used by the suspects to distribute illicit goods.
People engaging in facilitating activities are sometimes part of the social network of the suspects, but more often suspects or groups come into contact with these facilitators via the Internet. People who can hack systems, hosting providers, and advertising firms that place online advertisements containing concealed malware and ransomware sometimes offer their services on the Internet and can easily be found by anyone in need of such services. However, these facilitators are also found within the social network of the suspects. Friends, acquaintances and family members can become involved more or less wilfully in an organised crime network. Most facilitators become knowingly involved in criminal activities, but sometimes this happens involuntarily, and occasionally facilitators do not even know they are being exploited by the suspects to prepare their crimes.

Social opportunities via the Internet
Establishing contacts with people possessing the right skills is quite easy when it comes to cyber-related activities. The studied case files show that online communication platforms or forums appear to be important in establishing contacts needed to develop specific criminal activities. Sometimes existing or newly formed relationships give rise to joint criminal activities, but more often people planning a crime actively search for co-offenders with the right skills. These services are offered on a number of online cybercrime forums, where people present their particular specialisms. This leads to more opportunistic and less stable relationships between co-offenders, who just buy specific crime services when in need of them. Whether these facilitators should be seen as part of the crime group or the criminal network is a matter of perspective. Suspects seem to invest less in the relationships with co-offenders than appeared to be the case in traditional forms of organised crime, where co-offenders with specific skills were harder to find and where maintaining existing relationships for future activities was worth the effort.

Online cybercrime forums seem to provide a meeting place for criminals and function as communication channels. These forums enable groups to be globally located while working closely together, but suspects living close to each other also communicate via these channels. The channels are used for selling and sharing knowledge, software, scripts, goods, products and raw materials. The fact that online communication services mostly use encryption appears to be an important motivation to use these forums instead of more traditional communication channels.

New economic structures
Another important structural change associated with the use of the Internet is the way money can be transferred and laundered via the Internet. It is relatively easy

to shield global money transfers by using crypto currencies or money transfers via web accounts that are used as a bank account to pay money mules, for instance, and for the rental of servers. From the case files it was not possible to deduce how exactly the money is transferred and laundered in specific cases. However, it is obvious that the use of cryptocurrencies leads to new underground economic structures that are difficult to control. It would be interesting to examine to what extent rules, reporting systems and inspection bodies in the field of unusual transactions could also apply and be used for cryptocurrencies.

The organisation of cybercrime

Our cases show that suspects active in cybercrime work together with others. Cooperation with others makes it possible to use certain products (e.g. malware), skills (e.g. hacking), or connections (e.g. of a recruiter), or it is used to conceal certain activities or identities (e.g. using mules or cashers). This collaboration takes several forms. Suspects make use of each other's expertise (for example in writing or spreading viruses), which can result in a division of labour and the sharing of profits. Within this form of collaboration, the different suspects do not always have a common goal. Nonetheless, in other cases cooperating suspects do have a common goal, for example earning money by spreading ransomware, or setting up an illegal marketplace. Logically, the more successful the collaboration seems to be, the longer suspects tend to work together.

Our cases also show examples of ICT-skilled suspects working with other suspects, who at a certain point feel that they cannot refuse this, or who are threatened to commit certain cybercrimes.

These ways of cooperation are comparable to other forms of organised crime, as described in the Dutch Monitor on Organised Crime, where knowing and involving people with certain skills or connections is crucial (Kleemans et al., 2002; Van de Bunt et al., 2007; Kleemans & De Poot, 2008).

Striking similarities are:

- *Dynamic networks*: our cases show that criminal alliances are changeable. People get involved and people drop out. People sometimes also ally themselves with several others to commit different types of activities. They work, for example, together with person A to sell drugs online and with person B to sell them offline, or with person C to spread malware and with person D to commit (online) credit card fraud.
- *Based on social relationships*: in our cases family ties, friendships and exclusively online relationships all appear within collaborations. Online collaborators often regard one another as good acquaintances, even if known only by nicknames. They may well not know where their partner in crime is located, or even in what country. Chat sessions reveal suspects pointing out how long they have been in touch, which seems to imbue a sense of trust. Forums also play a role in the development of relationships.

There are also aspects of cyber-OC that seem to differ somewhat from other forms of organised crime:

- *Anonymity in cyberspace*: online activities may be conducted anonymously, and there is no need for offline contact between 'partners in crime' to commit online (criminal) activities. This makes cooperation less risky and changes the role of trust within criminal cooperation.
- *Crime-as-a-Service*: certain tasks can be bought online as services, which gives the organisation of cybercrime a new or different dimension. ICT-skilled people can sell their services to other online or offline active suspects. Within this 'cooperation', different individuals undertake specific activities and there is no real need

for them to make contact before the task is complete. Some create tools such as botnets or malware, others offer them for sale on cybercrime forums, a third party buys them and yet another actually uses them to cause damage or make money. In this scenario there does not have to be a sizable collaboration between the developer of, say, ransomware and the person who distributes it. However, there are cases in which someone who has created malware, for instance, actively seeks out people to disseminate it and makes an agreement with them to share the proceeds. Conversely, we also see individuals wishing to undertake criminal activities online going and searching for accomplices able to facilitate them, by hacking systems and stealing data.

- *Role of forums*: our cases show how illegal online marketplaces and forums facilitate the collaboration between suspects and lead to the formation of new collaborations between suspects active on these forums[42]. On closed forums, which can only be accessed with permission, suspects were active in the open section of a forum, but also communicated with a more select group of contacts 'behind closed doors'.

Long-term perspectives, chain structures, divided responsibilities: what's new?

Long-term perspective

The term 'organised crime' refers to both the complexity of the crime and *the long-term perspective* and the ability to conduct *ongoing criminal activities* of the groups or networks committing these crimes. Stable crime groups as well as fluid, changing criminal networks have proven to be able to commit such ongoing criminal activities with long-term prospects. The question is how this stability and long-term perspective relates to cyber-OC with its fluid online relationships.

The cases we studied show that crime groups that were already involved in organised crime before they 'entered the Internet' continue to operate within more or less the same organisational structure as before. These long-established group structures – either strictly organised or looser – seem to remain constant, even when these groups change their activities or expand to another type of crime. Although more technically skilled people may be involved, the core group of such collaboration seems to be rather stable and seems to keep this long-term perspective.

When it comes to newer crime groups emerging in the cyber field, this long-term perspective seems to take a different form. Although individuals seem to have a long-term perspective with regards to their own activities, the groups or networks that are involved in a particular crime are often less stable and do not always share this long-term perspective. Emerging crime groups can be active in certain collaborations for longer or shorter periods of time. Subjects involved in those crime groups seem to be less committed to engaging in long-term agreements with other members of the group. It seems to be less necessary as well, to form a stable group, because the trust between people involved in cyber-OC groups is less based on long-term cooperative relationships and more on the quality of their contribution. Suspects can maintain their anonymity in online collaborations. This makes online criminal collaboration less risky, and building trust less important in these cyber-OC groups.

As cyber-OC groups seem to be less dependent on the long-term commitment of the partners that contribute to a crime, this long-term perspective seems to become an individual choice or characteristic rather than a characteristic of this crime form.

[42] This is also recognised by Group IB, 2011 and Europol, 2015.

Offenders involved in cyber-OC create new marketplaces of subjects who can be hired for single specific occasions or for long-term involvement. Organised crime groups or networks operating in the cyber domain can use this marketplace either to recruit individuals with specific technical knowledge or to buy their services. Hence, they can continuously develop their criminal activities and make them technically more advanced.

The above-mentioned developments brought about crime groups or networks with new organisational structures, next to more traditional stable crime groups in the cybercrime domain. The organisational structures of the crime groups in the studied cases range from rather strictly organised groups to loosely organised networks. Within these loose networks the cooperation between suspects can take the form of a chain, linking people involved in different activities, which together constitute a criminal act.

Chain-structures and divided responsibilities
The chain-structures that characterise some of the analysed cyber-OC groups, entail other characteristics that affect the appearance of these forms of 'organised crime'. Therefore we elaborate a bit on this structural characteristic:

- In chain-like collaborations, suspects can get involved in organised crime without knowing exactly what they are involved in. This aspect is not new or striking for organised crime groups. There have always been suspects who were unaware of their involvement in organised crime. For security reasons, strictly organised crime groups often shield different activities or different parts of a group or network from each other. Suspects contributing to organised crime often do not have an overview of the crime they contribute to, and occasionally do not even know they are involved in a crime.
- Within a chain-structure, suspects work together, but are responsible for only a single part of a crime. Together, these different activities – which are separated in time and space, and are performed by different suspects – shape the crime as a whole. The whole does not exist without the pieces, and the value of the pieces cannot be assessed without taking the whole set of coherent activities into account. This feature is not new in organised crime either. In fact, it can be seen as a one of the defining features of organised crime. In strictly organised crime groups tasks are also often divided between different suspects, each of which is responsible for specific parts of a coherent set of activities. This can be achieved with various organisational structures. However in those cases there is always an intermediary who coordinates these different activities and who inspires confidence by guiding and controlling different suspects. Thanks to the Internet, the coordination of activities can now be achieved without an intermediary being aware of specific activities and of the ultimate goal.
- Within these chain-like structures, there is a fragmentation of the criminal act and often there even is an 'alienation' from this act, which leads to a shared responsibility where, in a way, every suspect has power, and every suspect has a certain role, but either everyone or no one seems to be responsible for the crime as a whole, and no one seems to have a clear view of the common goal they achieve by cooperating. Maybe there does not even have to be an intended goal. This seems to be quite a new characteristic of organised crime, manifesting itself in cyber-OC cases that we did not see before and that definitely changes our concept of what organised crime entails. In such a chain structure, the different players can all act for themselves and achieve private goals. Together they accomplish an organised form of crime, but that crime seems to arise bottom

up, rather than being organised top-down. This way, crimes as well as crime groups seem to more or less co-incidentally arise and take on a certain form.

Because of these developments cyber-OC can be committed either under mutual arrangements between offenders (suspects knowing each other and working together on a criminal project, relying on the division of tasks) or without any coordination in a chain environment. As a consequence, there is huge diversity and uncertainty, and it may become difficult to allocate crimes to specific crime groups or criminal organisations and to predict how crimes will take shape.

The concept of trust within cyber-OC

As mentioned previously, within these new crime groups, the concept of trust has acquired a different meaning (see also Lusthaus, 2012). In stable crime groups, trust is something that comes through long-term collaboration between people. Suspects participating in a crime group have to be loyal to the group. Trust ensures that crimes and identities of the group members remain hidden. However, in exchanges between cybercriminals this 'bonding capital' or 'thick trust' is not emphasized. Rather, their relationships are built on 'thin trust': weak ties that provide unique access to resources and opportunities outside their immediate social circles (Khodyakov, 2007). According to the literature, reputation is one of the primary tools for maintaining trust in the cyber world. Whereas thick trust is an important characteristic for criminal groups, thin trust is typical for virtual collaborations and for collaboration with experts outside people's own circles.

In the studied cyber-OC groups there were examples of traditional bonding and loyalty building mechanisms, like personal relationships, collaboration with trusted family members and friends, permanent personal contact, and power relations with threats and violence. But in other crime groups, especially those cooperating as looser networks with 'project-based' collaborations, trust seems to play a different role. Partners are selected based on reputation and previous accomplishments. Furthermore, the anonymity in cyberspace makes cooperation less risky and changes the way individuals participate in the criminal act. In looser networks, where offenders mainly know each other online, trust is a combination of prestige and reputation. Prestige comes with a certain skill set that can be used. Reputation is built through positive feedback from fellow criminals and customers. In these networks the meaning of trust has changed. Subjects trust each other in the anonymous context of the Internet and can share confidential matters there. This does however not mean that subjects would also trust each other in the offline world. The anonymity of the Internet seems to give subjects an adequate protection. This anonymous collaboration also influences the way in which power relations can be maintained and enforced, and agreements can be forced through treats. Physical violence makes way for cyber attacks. In the studied cases, trust seems to be measured by the skills and reputation of an individual, where reputation does not only refer to technical skills and fulfillment of agreements, but also to the way in which authority and cooperative behavior can be enforced.

Because skills become more important than loyalty, crime groups can operate in a more fragmented structure. This way, information about the criminal act as well as the perpetrators involved is more fragmented. Frequently, subjects involved in cyber-OC do not even know the real identity of their co-offenders. As a result, autonomous individuals are but a pawn in the entire scheme, with little information to give to the authorities.

Investigating and identifying suspects and criminal activities in cyberspace
Knowledge about the nature of organised forms of cybercrime can help law enforcement agencies to improve the prevention, investigation and prosecution of these complex crimes. In order to develop targeted prevention measures, a good understanding of the modus operandi of cybercrime groups is essential. Over the past ten years, substantial investments have been made to intensify law enforcement and criminal investigation on cybercrime. As a result the specialist team of the Dutch Police - the National High Tech Crime Unit - has grown rapidly in the last years. This means there is capacity and expertise reserved exclusively for addressing cybercrime cases. However, the amount of possible cybercrime cases the police become aware of is significant and even the capacity of the High Tech Crime Unit is limited. Due to resource considerations, the police are forced to fix priorities in detecting and investigating cases.
From the studied case files and interviews, it becomes clear that there is a wide array of sophisticated technical methods to act anonymously on the Internet. For police detectives this is a bottleneck and a challenge at the same time. The use of special investigative powers, appears to be effective in revealing someone's identity in some of the studied cases. These investigative powers can be applied both online and offline. For instance, the undercover agent acting online to eventually meet with a suspect in person. In other cases however, despite lots of effort made by the police, the team failed to find the person behind a nickname.
Another investigative power, the "old fashioned" telephone tap, still appeared to be surprisingly helpful in this digital era. The studied files contained a substantial amount of information that was intercepted with a telephone tap. Communication between people can contain valuable information about the way of cooperation. Conversations and messages between suspects cover useful information about their activities, contacts, lifestyle or motives. The casefiles also contained conversations between people held via online communication services. This information however, could only be read and studied on the computer or account of the suspect after the arrest. Besides the fact that online communication services are mostly located outside the Netherlands, these services are often encrypted and thereby not readable for the police with an Internet tap.
In several cases the police has confiscated data carriers, which are also often protected by strong encryption. The upcoming new Computer Crime Bill can offer the police new investigative tools, and creates possibilities to get access to information on these tools before it is encrypted.

Confiscation of assets
With regard to the challenges for law enforcement agencies in the case of cyber-OC, the detection and confiscation of assets from suspects appear to be a difficult or a time consuming part within the investigation. In only one case a separate financial investigation was started. In other cases large amounts of money are mentioned or seen on web accounts without knowing where it is or where it went. It appears that tracing criminal incomes is not an easy task, while the amounts of money in some cases are enormous. In the studied files, we found indications of money laundering via the Internet. Yet it is not entirely clear how this is done. It might be worth to invest in the knowledge about money flows on the Internet.

International cooperation
The Internet is a virtual place without borders, and criminal investigations concerning cyber-OC poses law enforcement agencies for new challenges. During the last decennium, substantial investments have been made in the Netherlands to intensify law enforcement on cybercrime. The investments have resulted in a constant

capacity of law enforcement agencies that is reserved to investigate cybercrime cases. However, since a criminal on the Internet can physically be anywhere; identifying, localising, arresting and finally convicting a criminal, often requires thorough international collaboration. This raises additional questions such as which country should prosecute the suspect because cybercrime has no strict geographical location.
Although the interviewees all spoke positively about the facilitating role of Europol within international cooperation, the success of Joint Investigation Teams appears to be heavily dependent on capacity and priorities in the collaborating countries. However, in police investigations that do not have the formal status of a JIT, formal requests to other jurisdictions are required for assistance or information. Due to different priorities, complicated paperwork or political difficulties, these requests are often dealt with a pace that is incompatible with the speed of the Internet. Overcoming these kinds of problems would be a real gain in the fight against major and important cybercriminals.

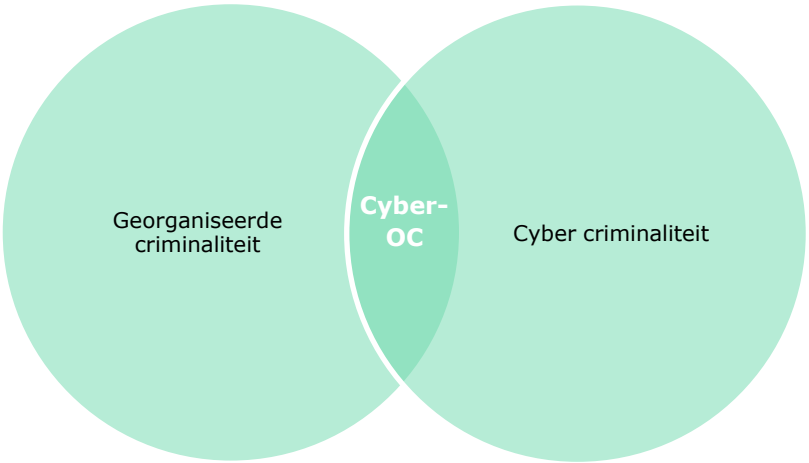
Final remark
Knowledge about the nature of cyber-OC can help law enforcement agencies to improve the prevention, investigation and prosecution of these complex crimes.
In order to develop targeted prevention measures, a good understanding of the modus operandi of cybercrime groups is essential. Therefore the further digitalisation process has to go hand-in-hand with a focus on the possible abuse of these systems and appropriately adapted built-in security and control mechanisms. At the same time it is important to update investigative measures and methods to keep up with the developments in cybercrime. The international characteristics of organised cybercrime require efficient possibilities for law enforcement agencies to collaborate instantly on an international level to keep up with the fluidity of the criminal groups and their activities. Knowledge about the nature of organised forms of cybercrime can help law enforcement to improve the prevention, investigation and prosecution of these complex crimes.
It is also necessary to understand how cyber-OC develops. Technological developments will further expand the possibilities to interact anonymously. Cybercriminals, evidence, profits and victims might become even more elusive than they already are. When different steps of an offence are committed by different people, as is the case in chain-like structures, it becomes difficult to understand the nature of a crime, to see how
crime develops, to identify those responsible for it, and to prevent, investigate and prosecute these crimes by traditional means.
Since the Internet is a virtual place without time, space, boundaries and jurisdiction, it requires creativity to apply existing investigative tools that are developed in an offline world to investigate severe forms of cyber-OC. For the prevention and repression of cyber-OC specific tools and new local and international laws seem to be necessary to open up the Internet to law enforcement.
This will be a challenge, because with new laws new privacy issues also arise that need to be considered. Governments will have to think creatively and collaboratively about new ways to combat these new forms of crime. Understanding how cyber-OC develops is a necessary first step. We hope this report has contributed to this goal.

Samenvatting

Georganiseerde Cybercrime in Nederland
Empirische bevindingen en implicaties voor de rechtshandhaving

Doel van het onderzoek

De toename van cybercriminaliteit en de verhoogde kwetsbaarheid om hier slachtoffer van te worden, is een zorg binnen de samenleving, van de rechtshandhaving en van beleidsmakers. Over de aard en de organisatie van deze criminaliteit is echter nog niet veel informatie beschikbaar. Dit onderzoek richt zich op de vraag hoe criminele samenwerkingsverbanden op, via en tegen het internet te werk gaan. We hebben ons daarbij gericht op kenmerken van de verdachten, hun organisatorische structuren en modus operandi. We hebben ook gekeken naar de manier waarop (georganiseerde) cybercriminaliteit wordt opgespoord en op de kansen en knelpunten die hierbij bestaan. Met de term 'cyber-OC' ofwel 'Cyber Organised Crime' (zie ook Bulanova-Hristova et al., 2016) doelen we op de overlap tussen de georganiseerde criminaliteit en cybercrime, met andere woorden, de *link* tussen en het samengaan van cybercrime en georganiseerde criminaliteit.



Andere doelstellingen van het onderzoek waren het verkennen van de volgende vragen: In hoeverre biedt het internet nieuwe 'windows of opportunity' voor illegale activiteiten en voor het vinden en benaderen van nieuwe slachtoffers?; In hoeverre heeft het internet geleid tot structurele veranderingen in de georganiseerde criminaliteit?

Onderzoeksmethoden: politiedossiers en interviews

Om de onderzoeksvragen te beantwoorden, zijn verschillende onderzoeksmethoden gebruikt. Er is een analyse gemaakt van politiedossiers van opsporingsonderzoeken naar georganiseerde cybercriminaliteit. Wij hebben hiervoor elf afgeronde opsporingsonderzoeken geselecteerd. De verdachten in deze zaken waren actief in ver-

schilende vormen van cybercriminaliteit: het verspreiden van malware, hacking, het runnen van botnets, phishing, misbruik van het bankwezen, het (digitaal) witwassen van geld en illegale online handel. Bijna alle zaken (tien) zijn inmiddels voor de rechter geweest en hebben geleid tot veroordelingen. Het opsporingsonderzoek van de onderzochte zaken heeft gelopen tussen 2009 en 2014. De politiedossiers van de elf opsporingsonderzoeken bevatten gegevens over in totaal 107 verdachten.
Naast de studie van politiedossiers, interviewden we twaalf functionarissen van politie en justitie om informatie te verzamelen. Dit betroffen officieren van justitie, politieagenten van de opsporingsteams, en vertegenwoordigers van de *Electronic Crimes Task Force* en van Europol. De gegevens zijn verzameld in het kader van een internationaal onderzoeksproject gefinancierd door de Europese Commissie (voor de eerdere publicatie op basis van deze data zie Bulanova-Hristova et al., 2016).[43]

Resultaten: de traditionele groepen en nieuwe allianties

In de geanalyseerde zaken zien we enerzijds traditionele criminele groepen die betrokken raken bij cybercrime om hun (traditionele) criminele activiteiten efficiënter of geavanceerder uit te voeren. Het gaat dan bijvoorbeeld om de online verkoop van drugs, of om het gebruik van het internet of encryptie bij hun 'interne' communicatie. Anderzijds zien we nieuwe groepen die specifieke cyber-gerelateerde criminele activiteiten ontwikkelen. Het gaat hier dus in feite om nieuwe vormen van criminaliteit, zoals DDoS-aanvallen, het verspreiden van malware en ransomware.

Nieuwe mogelijkheden: nieuwe ideeën, nieuwe slachtoffers

Ontwikkelingen op het gebied van internet en informatie- en communicatie technologieën zorgen voor nieuwe vormen en uitvoeringsmogelijkheden van criminaliteit. Het gaat dan bijvoorbeeld om anonimiteit, crime-as-a-service en de mogelijkheid om fora te gebruiken. Daarnaast zorgen deze ontwikkelingen voor nieuwe manieren om slachtoffers te bereiken; voor meer efficiëntie in de uitvoering; en voor een vergroting van de financiële opbrengst van criminaliteit. Deze ontwikkelingen zorgen ervoor dat criminaliteit waarbij coördinatie van verschillende activiteiten is vereist, in feite eenvoudiger en toegankelijker lijkt te zijn geworden voor grotere groepen mensen. Dit leidt, afgezien van veranderingen in de modus operandi en de veranderingen in de toegang tot slachtoffers, tot (1) nieuwe spelers in het veld, (2) nieuwe vormen van samenwerking en (3) nieuwe economische structuren.

1 Nieuwe faciliteerders

Een voorbeeld van nieuwe spelers zijn faciliteerders die bewust of onbewust en gewild of ongewild criminaliteit faciliteren. Zij bestaan onder meer uit technisch geschoolde mensen, en (legitieme) bedrijven (private partijen), zoals hosting providers, online reclamebureaus/advertentiebedrijven, webshops, koeriersbedrijven (postbedrijven) en telecommunicatiebedrijven. Daarnaast komen we faciliteerders tegen die helpen om zaken af te schermen, zoals dekmantel-ondernemingen, *bitcoin* handelaren en *money mules*. Deze faciliteerders zijn niet dezelfde partijen als partijen die actief zijn in offline georganiseerde misdaad. Deze nieuwe spelers bieden nieuwe mogelijkheden voor de aanpak en preventie van cybercrime en voor het

[43] EU Project: Bulanova-Hristova et al. (2016) (HOME/2012/ISEC/AG/4000004382).

betrekken van deze partijen, bijvoorbeeld binnen publiek-private samenwerkingsverbanden.

2 Samenwerking en organisatie

De manier waarop verdachten met elkaar samenwerken is voor een deel vergelijkbaar met andere vormen van georganiseerde misdaad. De overeenkomsten zijn:

- *Dynamische netwerken*: criminele samenwerkingsverbanden zijn veranderlijk qua samenstelling.
- *Gebaseerd op sociale relaties*: criminele samenwerkingsverbanden zijn gebaseerd op familiebanden, vriendschappen en andere offline en online relaties.

Er zijn ook aspecten van de georganiseerde cybercriminaliteit die enigszins verschillen van andere vormen van georganiseerde misdaad:

- *Anonimiteit in cyberspace*: online activiteiten kunnen anoniem worden uitgevoerd, en offline contact tussen 'partners in crime' is niet perse nodig om online (criminele) activiteiten te plegen. Dit maakt samenwerking minder risicovol en verandert de rol van vertrouwen binnen de criminele samenwerking.
- *Crime as a service*: bepaalde taken kunnen online worden gekocht als diensten, wat de organisatie van cybercrime een nieuwe of andere dimensie geeft. ICT-geschoolde mensen kunnen hun diensten verkopen aan anderen die online of offline actief zijn. Binnen deze 'samenwerking', ondernemen verschillende individuen specifieke activiteiten en er is geen echte noodzaak om offline contact met elkaar te hebben.
- *De rol van fora*: online fora waar wordt gecommuniceerd over cybercriminaliteit lijken te fungeren als ontmoetingsplaatsen en als communicatiekanalen voor het delen en verkrijgen van informatie en het leggen van contacten met betrekking tot criminele activiteiten (op het internet). Ze bevorderen de samenwerking tussen de verdachten en leiden tot de vorming van nieuwe samenwerkingen tussen verdachten die actief zijn op deze fora. Op deze manier kunnen verdachten online relaties opbouwen, samenwerken en communiceren zonder elkaar offline te hoeven ontmoeten. Deze kanalen worden gebruikt voor de verkoop en het delen van kennis, software, scripts, goederen, producten en ruw materiaal. Het feit dat online communicatiediensten encryptie gebruiken en de gebruiker vaak anoniem kan blijven door het gebruik van anonimiserings-software, blijkt een belangrijke motivatie te zijn om deze fora te gebruiken in plaats van meer traditionele communicatiekanalen.

Ketenstructuren: verdeelde verantwoordelijkheden en de rol van vertrouwen

Verder lijken nieuwere groepen binnen cybercriminaliteit, in tegenstelling tot de meer traditionele georganiseerde misdaad groepen, te verschillen als het gaat om hun lange termijn perspectief binnen de samenwerking. Hoewel individuen wel een lange termijn perspectief hebben ten aanzien van hun eigen activiteiten, zijn de nieuwe samenwerkingsverbanden vaak minder stabiel en kennen zij in mindere mate een lange termijn perspectief ten aanzien van het gezamenlijk uitvoeren van illegale activiteiten. Anders dan bij traditionele georganiseerde criminaliteit waar vertrouwen tussen samenwerkende verdachten een belangrijke rol speelt, lijkt het bij online samenwerkingsverbanden minder noodzakelijk te zijn om een stabiele groep te vormen. De kwaliteit van iemands kennis en kunde speelt een belangrijkere rol. De anonimiteit van online samenwerking, maakt deze samenwerking minder riskant, waardoor het opbouwen van vertrouwen tussen verdachten binnen deze cyber-OC-groepen minder belangrijk is. Binnen deze lossere netwerken kan samenwerking tussen verdachten de vorm hebben van een keten, waarbinnen mensen die betrokken zijn bij verschillende activiteiten aan elkaar gekoppeld zijn,

en waarvan de verschillende activiteiten samen een strafbaar feit opleveren. In deze keten-achtige samenwerkingen, werken verdachten wel met elkaar samen, maar zijn zij slechts verantwoordelijk voor één onderdeel van de criminele activiteit. Als gevolg hiervan kunnen verdachten betrokken zijn bij georganiseerde criminaliteit, zonder precies te weten van welke misdaden hun activiteiten onderdeel uitmaken. Binnen deze keten-achtige structuren heeft elke verdachte in zekere zin macht, en elke verdachte heeft een bepaalde rol, maar tegelijkertijd lijkt iedereen of juist niemand verantwoordelijk te zijn voor de misdaad als geheel. Dit lijkt een nieuw kenmerk van georganiseerde criminaliteit op het terrein van cybercrime, wat een verandering zou betekenen voor de inhoud van het concept georganiseerde criminaliteit. In zo'n ketenstructuur kunnen de verschillende spelers voor zichzelf bezig zijn en individuele doelen hebben. Samen bereiken ze een georganiseerde vorm van criminaliteit, niet zozeer van bovenaf georganiseerd maar veeleer bottom-up ontstaan. Op deze manier lijken zowel de criminele activiteiten als de groepen van samenwerkende personen min of meer op toevallige wijze te ontstaan en bepaalde vormen aan te nemen.

Deze ontwikkelingen maken dat cyber-OC zowel kan worden gepleegd op basis van onderlinge afspraken tussen verdachten (die elkaar kennen en samenwerken aan een bepaald project, op basis van een bepaalde verdeling van taken) of juist in de vorm van de hierboven geschetste ketenstructuur, dus zonder duidelijke coördinatie. Er bestaat dus diversiteit waardoor het moeilijk kan zijn om criminaliteit aan specifieke criminele groepen of organisaties toe te wijzen en om te voorspellen hoe criminaliteitsvormen zich ontwikkelen.

3 Nieuwe economische structuren

Het gebruik van cryptocurrencies om geld te versturen of om geld wit te wassen via het internet hebben geleid tot het ontstaan van nieuwe economische structuren. Deze nieuwe vormen van ondergronds bankieren vormen structuren die moeilijk te controleren zijn. Het is interessant om na te gaan in hoeverre regels, meldingssystemen en controlerende instanties op het gebied van ongebruikelijke transacties ook gelden en gebruikt kunnen worden voor cryptocurrencies.

De opsporing van georganiseerde cybercriminaliteit

Het speciale cybercrime team van de Nederlandse Politie – het Team High Tech Crime – is de afgelopen jaren hard gegroeid. Dit betekent dat capaciteit en expertise is vrijgemaakt en gereserveerd voor de opsporing van cybercrime zaken. Cybercrime neemt echter toe en de politie is genoodzaakt om prioriteiten te stellen bij het signaleren en opsporen van zaken.

Bijzondere opsporingsbevoegdheden

Het brede scala aan geavanceerde technische mogelijkheden om anoniem te handelen op het internet, maken dat bijzondere opsporingsbevoegdheden worden ingezet om de identiteit van verdachten te kunnen achterhalen. Deze opsporingsbevoegdheden worden zowel online als offline toegepast. Het nieuwe wetsvoorstel Computercriminaliteit III biedt de politie nieuwe onderzoeksinstrumenten, en creëert mogelijkheden om de toegang tot informatie te krijgen voordat de informatie gecodeerd wordt.

Informatiepositie op internet
Om grip te krijgen op traditionele georganiseerde criminele groepen, beschikt de Nederlandse politie over een speciale eenheid, de Criminele Inlichtingen Eenheid (CIE). Rechercheurs van de CIE kunnen undercover samenwerken met mensen in een criminele groep en op deze manier informatie vergaren over criminele activiteiten. Deze informatie wordt vaak gebruikt als een startpunt voor een strafrechtelijk onderzoek. Een soortgelijke eenheid voor de online criminele wereld bestaat echter nog niet. Als gevolg daarvan heeft het Team High Tech Crime nog geen vergelijkbare informatiepositie in de internetgemeenschap. Verschillende geïnterviewden zijn van mening dat de ontwikkeling van een dergelijke informatiepositie in de toekomst waardevol zou zijn in de strijd tegen cybercriminaliteit.

Internationale samenwerking
Aangezien een verdachte op het internet zich overal ter wereld kan bevinden, vergt het identificeren, lokaliseren, arresteren en uiteindelijk veroordelen van verdachten vaak een intensieve internationale samenwerking. Onze geïnterviewden zijn positief over de faciliterende rol van Europol bij internationale samenwerking, al lijkt het succes van Joint Investigation Teams sterk afhankelijk van de capaciteit en prioriteiten in de samenwerkende landen. Binnen politie onderzoeken die niet de formele status van een JIT hebben, zijn rechtshulpverzoeken nodig om hulp of informatie te krijgen uit andere jurisdicties. Door verschillende prioriteiten, ingewikkeld papierwerk of procedures, worden deze verzoeken vaak behandeld met een tempo dat onverenigbaar is met de snelheid van het internet. Het overwinnen van dit soort problemen zou winst kunnen opleveren in de opsporing van (georganiseerde) cybercrime.

References

Adams, S.A., Brokx, M., Dalla Corte, L., Galic, M., Koops, B.-J., Leenes, R., Schellekens, M., E Silva, K., & Skorvánek, I. (2015). *The governance of cybersecurity. A comparative quick scan of approaches in Canada, Estonia, Germany, the Netherlands and the UK.* Tilburg: TILT.

Beijer, A., Bokhorst, R.J., Boone, M., Brants, C.H., & Lindeman, J.M.W. (2004). *De wet bijzondere opsporingsbevoegdheden:Eindevaluatie*. The Hague: Boom. Onderzoek en beleid 222.

Bernaards, F, Monsma, E., & Zinn, P. (2012). *Criminaliteitsbeeldanalyse High Tech Crime* (CBA). KLPD: Woerden.

Bokhorst, R.J., Van der Steeg, M., & Poot, C.J. de (2011). *Rechercheprocessen bij de bestrijding van georganiseerde criminaliteit*. The Hague: WODC. Cahier 2011-11.

Bulanova-Hristova, G., Kasper, K., Odinot, G., Verhoeven, M., Pool, R., Poot, C. de, Werner, W., & Korsell, L. (Eds.)(2016). *Cyber-OC - Scope and manifestations in selected EU member states.* Wiesbaden : Bundeskriminalamt.

Council of Europe (2001). *Convention on cybercrime*, Budapest, 23.XI.2001. European Treaty Series, No. 185*.* Accessed 09.04.2015: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/T-CY/Default_TCY_en.asp.

Council of the European Union (CotEU 2015). *Evaluation report on the seventh round of mutual evaluations 'The practical implementation and operation of European policies on prevention and combating Cybercrime': Report on the Netherlands.* Brussels: CotEU.

De Cuyper, R.H., & G. Weijters (2016). *Cybercrime in cijfers: Een verkenning van de mogelijkheden om cybercrime op te nemen in de Nationale Veiligheidsindices*. The Hague: WODC. Memorandum 2016-1.

De Graaf, D., Sosha, A.F., Gladyshev, P. (2013). Bredolab: Shopping in the cybercrime underworld. In M. Rogers & K.C. Seigfried-Spellar (Eds.), *Digital Forensics and Cybercrime: 4th International Conference ICDF2C 2012* (pp. 302-313). Berlin/New York: Springer.

Dienst Landelijke Recherche & Landelijk Parket (2014). *Tactische Programma High Tech Crime 2014*. S.l.: S.n.

Dietrich, D., Kasper, K., Bulanova-Hristova, G. (2016). Literature review. In G. Bulanova-Hristova et al (Eds). *Cyber-OC: Scope and Manifestations in selected EU member states.* Wiesbaden: Bundeskriminalamt.

Electronic Crimes Task Force (ECTF) (2011). *Covenant Samenwerking en informatie-uitwisseling Electronic Crimes Task Force*. www.rijksoverheid.nl/documenten/convenanten/2011/03/15/convenant-samenwerking-en-informatie-uitwisseling-electronic-crimes-task-force.

Europol (2015). *The Internet Organised Crime Threat Assessment (IOCTA) 2015*. S.l.: Europol.

Eurojust (2015). *Report of the Strategic Meeting on Cybercrime November 2014: Task Force on Cybercrime*. S.l.: Eurojust.

Ferdinandusse, W. N., Laheij, D., & Hendriks, J. C. (2015). *De bewaarplicht telecomgegevens en de opsporing: Het belang van historische telecommunicatie gegevens voor de opsporing.* S.l.: Politie/Openbaar Ministerie.

Group IB (2011). *State and rends of the 'Russian' Digital Crime Market.* Accessed 30.03.2015: www.group-ib.com/images/media/Group-IB_Report_2011_ENG.pdf.

Hulzebosch, B., & Van Velzen, A. (2015). *Inventarisatie en classificatie van standaarden in cybersecurity*. Enschede: Innovalor.

Inspectie Openbare Orde en Veiligheid (2012). *Follow the money!* The Hague: IOOV.
Kaspersen, H.W.K. (1990). S*trafbaarstelling van computermisbruik*. Deventer: Kluwer.
Kaspersen, H.W.K. (2004). Bestrijding van cybercrime en de noodzaak van internationale regelingen. *Justitiële Verkenningen*, (8), 58-75.
Kaspersen, H.W.K. (2006). Jurisdiction in the Cybercrime Convention. In E.J. Koops & S. Brenner (Eds.), *Cybercrime and Jurisdiction: A Global Survey.* The Hague: West Nyack.
Khodyakov, D. (2007). Trust as a process: A three-dimensional approach. *Sociology*, *41*, 115-132.
Kleemans, E.R., Berg, E.A.I.M. van den, & Bunt, H.G. van de, m.m.v. Brouwers, M., Kouwenberg, R.F., & Paulides, G. (1998). *Organized crime in the Netherlands: Report based on the WODC-monitor* [English summary]. The Hague: WODC. Onderzoek en beleid 173.
Kleemans, E.R., M.E.I. Brienen, H.G. van de Bunt, m.m.v. R.F. Kouwenberg, G. Paulides, J. Barensen (2002). *Georganiseerde criminaliteit in Nederland: Tweede rapportage op basis van de WODC-monitor*. The Hague: WODC. Onderzoek en beleid 198.
Kleemans, E.R., C.J. De Poot (2008). Criminal Careers in Organized Crime and Social Opportunity Structure. *European Journal of Criminology 5*(1), 69-98.
Klip, A.H. (2000). Soevereiniteit in het strafrecht. In G.J.M. Corstens & M.S. Groenhuijsen (Eds.), *Rede en Recht: Opstellen ter gelegenheid van het afscheid van prof. mr. N. Keijzer van de Katholieke Universiteit Brabant.* Deventer: Gouda Quint.
Koops, B.J. (Ed.) (2007). *Strafrecht en ICT*. The Hague: SDU Uitgevers.
Koops, B.J. (2010). Cybercrime Legislation in the Netherlands. In J.H.M. Van Erp & L.P.W. van Vliet (Eds.), *Netherlands Reports to the Eighteenth International Congress on Comparative Law.* Antwerp: Intersentia.
Koops, B.J. (2010). The Internet and its opportunities for cybercrime. In M. Herzog-Evans (Ed.), *Transnational Criminology Manual* (pp. 735-754). Nijmegen. Wolf Legal Publishers.
Koops, B.J. (2012). De dynamiek van cybercrimewetgeving in Europa en Nederland. *Justitiële Verkenningen*, (1), 9-24.
Koops. B.J. & Buruma, Y. (2007). Formeel strafrecht en ICT. In Koops, E.J. (Ed.), *Srafrecht & ICT* (2nd edition). The Hague: Sdu Uitgevers. Monografieen Recht en Informatietechnologie, no. 1.
Koops, B.J., & Goodwin, M. (2014). *Cyberspace, the cloud, and cross-border criminal investigation.* Tilburg: TILT.
Koops, B., Leenes, R., De Hert, P., & Olislaegers, R. (2012). *Misdaad en opsporing in de wolken: Knelpunten en kansen van cloud computing voor de Nederlandse opsporing.* Tilburg: TILT.
Kop, N. (2012). Criminele Inlichtingen Eenheden: dilemma's en kansen. *Tijdschrift voor de Politie*, *74*(1), 6-10.
Kop, N. & Giels, B. van (2011). *Bundeling van kracht: over professionalisering, presterend vermogen en (bovenregionale) samenwerking van de CIE.* Vertrouwelijk. Apeldoorn: Politieacademie.
Krommendijk, M., Terpstra, J., & Van Kempen, P. H. (2009). *De Wet BOB: Titels IVa en V in de praktijk. Besluitvorming over bijzondere opsporingsbevoegdheden in de aanpak van georganiseerde criminaliteit.* The Hague: Boom.
Kruisbergen, E.W., & Jong, D. de, with Kouwenberg, R.F. (contrib.) (2010). *Opsporen onder dekmantel.* The Hague: Boom Juridische uitgevers. Onderzoek en beleid 282.

Kruisbergen, E. W., Bunt, H. G. van de, and Kleemans, E. R. (2012). *Georganiseerde criminaliteit in Nederland: Vierde rapportage op basis van de Monitor Georganiseerde Criminaliteit*. The Hague: Boom Lemma. Onderzoek en beleid 306.

Kruithof, K., Aldridge, J., Décary-Hétu, D., Sim, M., Dujso, E., Hoorens, S (2016). *Internet-facilitated drugs trade. An analysis of the size, scope and the role of the Netherlands.* RAND Europe/WODC.

Kruse, W.G. & Heiser, J.G. (2002). *Computer forensics: incident response essentials.* Addison-Wesley.

Landelijk Parket (2014). *Tactische Programma High Tech Crime 2014.* Dienst Landelijke Recherche.

Lakerveld, J.A. van, Broek, S.D., Buiskool, B.J., Grijpstra, D.H., Gussen, I., Tönis, I.C.M., Zonneveld, C.A.J.M. (2014). *Arbeidsmarkt voor cyber security professionals.* Leiden: Plato.

Leukfeldt, E.R. (2014). Cybercrime and social ties. Phishing in Amsterdam. *Trends in Organised Crime*, *17*, 231-249.

Leukfeldt, R. (2015) Organised cybercrime and social opportunity structures: A proposal for future research directions. *The European Review of Organised Crime, 2*(2), 91-103.

Leukfeldt, R. (2016). *Cybercriminal networks: origin, growth and criminal capabilities*. The Hague: Eleven International Publishing. (phd-thesis)

Leukfeldt, R. & Yar (2016). Applying routine activity theory to cybercrime. A theoretical and empirixal analysis. *Deviant Behavior*, 37, 263-280.

Leukfeldt, R., Kleemans, E.R. & Stol, W. (2016). Cybercriminal networks, social ties and online forums: social ties versus digital ties within phishing and malware networks. *British Journal of Criminology* (February 2016).

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

McAfee Center for Strategic and International Studies (2014). *Net losses: estimating the Global Cost of Cybercrime.* Santa Clara, CA: McAfee. www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf

McGuire, M. & Dowling, S. (2013). Cyber crime: A review of the evidence. *Research report 75*. London.

Ministerie van Veiligheid en Justitie (2014). *Veiligheidsagenda 2015–2018.* The Hague: Min. VenJ.

NCTV – National Coordinator for Security and Counterterrorism (2013). *NCSS – National Cyber Security Strategy 2*. The Hague: NCTV. www.nctv.nl/Images/ncss-2-webversie-def_tcm126-519975.pdf.

Nelen, H. (2004). Hit them where it hurts most? The proceeds-of-crime approach in the Netherlands. *Crime, Law and Social Change* 41(5): 517-534.

Nelen, J. M., & Sabee, V. (1998). *Het vermogen te ondernemen: Evaluatie van de ontnemingswetgeving – Eindrapport.* The Hague: WODC. Onderzoek en beleid 170.

Odinot, G., Jong, D. de, Leij, J.B.J. van der, Poot, C.J. de, & Straalen, E.K. van (2012). *Het gebruik van de telefoon- en internettap in de opsporing.* The Hague: Boom Lemma. Onderzoek en beleid 304.

Odinot, G., Jong, D. de, Bokhorst, R. J., & Poot, C.J. de (2013). *The Dutch implementation of the Data Retention Directive*. The Hague: Eleven International Publishing. Onderzoek en beleid 310a. https://english.wodc.nl/onderzoeksdatabase/ov-201402-the-dutch-implementation-of-the-data-retention-directive.aspx.

Oerlemans, J.J. (2010). Het conceptwetsvoorstel versterking bestrijding computercriminaliteit nader bezien. *Tijdschrift voor Internetrecht,* (5), 148-152.

Oerlemans, J.J. (2011). Hacken als opsporingsbevoegdheid. *Delikt en Delekwent,* (62), 888-908.
Oerlemans, J.J, Custers, B.H.M., Pool, R.L.D., & Cornelisse, R. (2016). *Cybercrime en witwasssen.* The Hague: Boom criminologie. Onderzoek en beleid 319.
Openbaar Ministerie (2015). *OM Meerjarenplan Cybercrime 2015–2018*. S.l.: S.n.
Richet, J. (2013). From Young Hackers to Crackers. *International Journal of Technology and Human Interaction, 9*(3), 53-62.
Scheepmaker, M. (Ed.) (2004). Cybercrime. *Justitiële verkenningen, 30*(8).
Scheepmaker, M. (Ed.) (2012). Themanummer Veiligheid in cyberspace. *Justitiële verkenningen, 38*(1).
Stol, W.Ph., Leukfeldt, E.R., & Klap, H. (2012). Cybercrime en politie: Een schets van de Nederlandse situatie anno 2012. *Justitiële verkenningen*, *38*(1), 25-39.
Struiksma, N., De Vey Mestdagh, C.N.J., & Winter, H.B. (2012). *De organisatie van de opsporing van cybercrime door de Nederlandse politie*. Amsterdam: Reed Business.
Tak, P.J.P (2008). *The Dutch Criminal System* (3e ed.). Nijmegen: Wolf Legal Publishers.
Van de Bunt, H.G., & Kleemans, E.R., with the cooperation of De Poot, C.J., Bokhorst, R.J., Huikeshoven, M., Kouwenberg, R.F., Van Nassou, M., & Staring, R. (2007). *Organized crime in the Netherlands: Third report of the organized crime monitor* [English summary]. The Hague: Boom Juridische Uitgevers. Onderzoek en beleid 252.
Van den Broek, T.C. Weijters, G., & Van der Laan, A.M. (2014). *Antisociaal gedrag van jongeren online.* The Hague: WODC. Factsheet 2014-1.
Van der Hulst, R., & Neve, R. (2008). *High-tech crime, soorten criminaliteit en hun daders: Een literatuurinventarisatie.* The Hague: Boom Juridische uitgevers. Onderzoek en beleid 264.
Van der Meulen, N. (2015). *Investeren in Cybersecurity*. Cambridge: RAND Europe.
Van der Laan, A.M., & Goudriaan, H. (2016) *Monitor jeugdcriminaliteit: Ontwikkelingen in de jeugdcriminaliteit tussen 1997 en 2015.* The Hague: WODC. Cahier 2016-1.
Van der Leij, J.B.J. (2014). Het Nederlandse strafrechtssyteem. In Criminaliteit en Rechtshandhaving 2013, Ontwikkelingen en samenhangen. The Hague: Boom Lemma. Justitie in statistiek 4.
Van der Meulen, N. (2015). *Investeren in Cybersecurity.* Cambridge: RAND Europe.
Van Koppen, M.V., De Poot, C.J., Kleemans, E.R., & Nieuwbeerta, P. (2010). Criminal trajectories in organized crime. *The British Journal of Criminology*, *50*(1), 102-123.
Van Wingerde, K., & Van de Bunt, H. (2016) Geëiste en opgelegde sancties bij de strafrechtelijke afhandeling van georganiseerde criminaliteit. *Tijdschrift voor Criminologie*, *58*(2), 19-35.
Verhoeven, M., Van Gestel, B., & De Jong, D. (2011). *Mensenhandel in de Amsterdamse raamprostitutie: Een onderzoek naar de aard en opsporing van mensenhandel.* The Hague: Boom Juridische uitgevers. Onderzoek en beleid 295.
Wall, D. (2010). Criminalising cyberspace: The rise of the Internet as a 'crime problem'. In Y. Jewkes & M. Yar (Eds.), *Handbook of Internet crime.* Cullompton: Willan Publishing.
Wall, D.S. (2005). The Internet as a conduit for criminals. In A. Pattavina (Ed.), *Information Technology and the criminal justice System* (pp. 77-98). Thousand Oaks, CA: Sage.
Wall, D.S. (2014). *High risk cybercrime is really a mixed bag of threats*. Retrieved May 2016 from: http://theconversation.com/high-sisk-cyber-crime-is-really-a-mixed-bag-of-threats-34091

Wervingsfolder Politie 2013.
Wiemans, F.P.E. (2004). *Onderzoek van gegevens in geautomatiseerde werken* (Dissertation, Tilburg University). Nijmegen: Wolf Legal Publishers.
Zebel, S., De Vries, P., Giebels, E., Kuttschreuter, M., & Stol, W. (2013). *Jeugdige daders van cybercrime in Nederland*. Enschede: Universiteit Twente.

Case law

Hoge Raad 11 October 2005, *LJN* AT4351.
Hof 's-Gravenhage, 27 April 2011, *LJN* BR6836.
Rechtbank Den Haag 11 March 2015, ECLI:NL:RBDHA:2015:2498.
Rechtbank Rotterdam 26 March 2010, *LJN* BM2520.

Parliamentary papers

Kamerstukken II [Dutch parliamentary document] 2004/05, 26 671, no. 10.
Kamerstukken II [Dutch parliamentary papers] 2013–2014, 33 930 VI, no. 1.
Kamerstukken II [Dutch parliamentary document] 2015/16, 34 372, no. 4.
Kamerstukken II [Dutch parliamentary document] 2015/16, 34 372, no. 3.
Kamerstukken II [Dutch parliamentary papers] 2014-2015, 286.
https://zoek.officielebekendmakingen.nl/kv-tk-2014Z14361.html

Web links

Convention on Cybercrime, par. 193. www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures
www.dutchcowboys.nl/cybercrime/politie-en-cybercriminelen-zijn-op-zoek-naar-medewerkers-met-dezelfde-vaardigheden
http://computerworld.nl/beveiliging/79823-torrat-bende-anoniem-door-gebruik-vpn-en-bitcoins.
www.bbc.com/news/technology-18189987
www.huffingtonpost.com/2012/05/24/georgy-avanesov-found-guilty_n_1543687.html
http://krebsonsecurity.com/2010/10/bredolab-mastermind-was-key-spamit-com-affiliate/