



Bundeskriminalamt



Wetenschappelijk Onderzoek- en
Documentatiecentrum
Ministerie van Veiligheid en Justitie

Edited by
Gergana Bulanova-Hristova
Karsten Kasper
Géralda Odinet
Maite Verhoeven
Ronald Pool
Christianne de Poot
Yael Werner
Lars Korsell

Cyber-OC – Scope and manifestations in selected EU member states



This project has been funded with support from the European Commission. This publication reflects the views only of the authors, and the European Commission cannot be held responsible for any use which may be made of the information contained therein.

Cyber-OC – Scope and manifestations in selected EU member states



This project has been funded with support from the European Commission. This publication reflects the views only of the authors, and the European Commission cannot be held responsible for any use which may be made of the information contained therein.

Polizei + Forschung

Volume 50

Published by the
Bundeskriminalamt
Criminalistic Institute

BJA Advisory Board:

Professorin Dr. Regina Ammicht Quinn
Universität Tübingen, Internationales Zentrum für Ethik in den Wissenschaften

Professor Dr. Johannes Buchmann
Direktor des Center for Advanced Security Research Darmstadt

Professorin Dr. Petra Grimm
Hochschule der Medien Stuttgart

Professorin Dr. Rita Haverkamp
Universität Tübingen, Stiftungsprofessur für Kriminalprävention und
Risikomanagement

Professor em. Dr. Hans-Jürgen Kerner
Universität Tübingen, Institut für Kriminologie

Uwe Kolmey
Präsident des Landeskriminalamtes Niedersachsen

Professor Dr. Hans-Jürgen Lange
Präsident der Deutschen Hochschule der Polizei

Professor Dr. Peter Wetzels
Universität Hamburg, Fakultät für Rechtswissenschaft, Institut für Kriminologie

Klaus Zuch
Senatsverwaltung für Inneres und Sport Berlin

Edited by

Gergana Bulanova-Hristova

Karsten Kasper

Geralda Odinet

Maite Verhoeven

Ronald Pool

Christianne de Poot

Yael Werner

Lars Korsell

Cyber-OC – Scope and manifestations in selected EU member states

(HOME/2012/ISEC/AG/4000004382)



This project has been funded with support from the European Commission. This publication reflects the views only of the authors, and the European Commission cannot be held responsible for any use which may be made of the information contained therein.

**Bibliographical data of the Deutsche Nationalbibliothek
(German National Library)**

The German National Library catalogues this publication in the German National Bibliography; detailed bibliographical data will be available on the internet under <http://dnb.d-nb.de>.

Project Management:

BKA

Dr. Heinz Büchler, Head of IZ 34 – Research and Advisory Unit for Organised Crime,
Economic Crime and Crime Prevention

Project team:

BKA

Dr. Gergana Bulanova-Hristova

Karsten Kasper, M.A.

Gerhard Flach, First Detective Chief Inspector (EKHK)

Brå

Yael Werner, M.Sc.

Dr. Lars Korsell

WODC

Dr. Geralda Odinet

Maite A. Verhoeven, M.Sc.

Ronald L. D. Pool, LL.M.

Prof. Dr. Christianne J. de Poot

Project financial management:

BKA

Martin Löbke, Detective Chief Inspector (KHK)

All rights reserved

© 2016 Bundeskriminalamt Wiesbaden, Brottsförebyggande rådet, Wetenschappelijk Onderzoek- en Documentatiecentrum

This work is copyrighted in its entirety. Any usage in violation of the narrow boundaries of copyright law without the prior approval of the publisher is prohibited and is punishable by law. This especially applies for duplications, translation, microfilms, other types of processing, as well as for the storing and processing in electronic systems.

Editorial Office: Wissenschaftslektorat Zimmermann, Magdeburg

Production: Griebisch und Rochol Druck GmbH, Hamm

Contents

I. Introduction

<i>The project team</i>	1
1 Background	2
2 Project objectives and research questions	3
3 Definitions	4
4 Methodology	7
4.1 Literature review	9
4.2 Empirical data collection	10
4.3 Common checklist	11
4.4 Common analysing system	12

II. Cyber-OC in the Netherlands

<i>G. Odinot, M.A. Verhoeven, R.L.D. Pool, C.J. de Poot</i>	15
1 Organisation of investigation and prosecution in the Netherlands .	16
1.1 Criminal investigation of cybercrime in the Netherlands . . .	18
1.2 Legal framework on cybercrime in the Netherlands	23
2 Methodology	33
2.1 Selection of Dutch cases	33
2.2 Information available in police files	34
2.3 Interviews with experts	34
3 General description of the Dutch sample	35
4 Empirical findings	38
4.1 Suspect characteristics	38
4.2 Activities and modi operandi in the field of Cyber-OC	45
4.3 Collaboration and organisation	57
4.4 Damage of Cyber-OC	63
4.5 Criminal investigation of Cyber-OC	64
5 Concluding remarks for the Netherlands	88
6 References	95

III. Cyber-OC in Sweden

<i>Y. Werner, L. Korsell</i>	101
1 Context information	103
1.1 The character of cybercrime in Sweden	103
1.2 Development over time	103
1.3 Swedish penal legislation	104
1.4 Statistics	105
1.5 Political agenda	107
1.6 The police organisation	108
1.7 Measures by the police	109
2 Methodology	110
2.1 Selection of cases	110
2.2 Information available in police or prosecution files	110
2.3 Expert interviews	111
2.4 The cases	111
3 General description of the Swedish sample	112
3.1 Visible characteristics	112
3.2 Invisible characteristics	114
3.3 Typology	115
4 Empirical findings	118
4.1 Characteristics of suspects and groups in Cyber-OC	119
4.2 Activities and modi operandi in the field of Cyber-OC	127
4.3 External cooperation in the field of Cyber-OC	134
4.4 Summary suspects, groups, modi operandi and cooperation	137
4.5 Damage of Cyber-OC	138
4.6 Criminal investigation of Cyber-OC	140
5 Concluding remarks for Sweden	155
5.1 Involvement of OC in cybercrime	155
5.2 Using the internet to commit offline OC	157
5.3 Windows of opportunity for OC groups	157
5.4 Structural changes in OC	159
5.5 The organisation of cybercrime	160
5.6 Recommendations	160
6 References	162

IV. Cyber-OC in Germany

<i>G. Bulanova-Hristova, K. Kasper</i>	165
1 Context information	167
2 Methodology	169
2.1 First inquiry – focus on criminal groups	170
2.2 Second inquiry – focus on cybercrime	171
2.3 Sampling	172
3 General description of the reported criminal investigations	173
3.1 Activity fields	174
3.2 Suspects and damage	175
4 Empirical findings	177
4.1 Overview of the sample	177
4.2 Group categorisation	178
4.3 Determination of the group membership	180
4.4 Summary of the analysed investigations	181
4.5 Characteristics of Cyber-OC suspects	185
4.6 Characteristics of Cyber-OC groups	195
4.7 Activities and modi operandi in the field of Cyber-OC	205
4.8 Damage of Cyber-OC	206
4.9 Investigative measures in the analysed Cyber-OC cases	212
5 Concluding remarks for Germany	213
5.1 Answers to the research questions	213
5.2 Key findings of the German case study	216
6 References	217

V. Concluding remarks from the three case studies

<i>The project team</i>	221
Theme 1: Organised crime groups entering cyberspace	223
Theme 2: Structure and organisation	224
Theme 3: Trust	226
Theme 4: Cyberspace and cyber logistics	228
Theme 5: Initiation of crimes and crime groups	229

Theme 6: New windows of opportunity	231
Theme 7: Long-term activities	232
Theme 8: The term ‘organised crime’	234
Final remark	236

VI. Appendix – Literature review

<i>Dorothee Dietrich, Karsten Kasper, Gergana Bulanova-Hristova . . .</i>	239
---	-----

Figures and Tables

Figure 1: Suspects by primary role	38
Figure 2: Suspects by age	40
Figure 3: Suspects with criminal history	41
Figure 4: Criminal history of suspects	42
Figure 5: Reported crimes	106
Figure 6: Hierarchic group structure	121
Figure 7: Network of clusters	125
Figure 8: Division of criminal investigations into cybercrime in a narrow/broad sense (N = 128)	174
Figure 9: Distribution of the criminal investigations to different crime areas (N = 128)	175
Figure 10: Distribution of criminal investigations according to area of crime (N = 18)	177
Figure 11: Matrix of group categories in Cyber-OC	178
Figure 12: All identified suspects per group	185
Figure 13: Number of core group members in comparison with total suspects (categories 1 and 2)	186
Figure 14: Distribution of gender (all identified suspects)	187
Figure 15: All identified suspects by age	188
Figure 16: Average age of suspect categories	189

Figure 17:	Distribution of suspects according to age classes	190
Figure 18:	Average age per group	191
Figure 19:	Cyber-OC groups with a homogeneous core group (n = 9)	193
Figure 20:	Formation process of cyber-entering groups	197
Figure 21:	Formation process of offlineborn groups	198
Figure 22:	Formation process of cyberborn groups	199
Figure 23:	composition of core groups and peripheries of selected groups	201
Figure 24:	Example of hierarchic group structure	202
Figure 25:	Financial damage in the analysed Cyber-OC cases	208
Table 1:	Public Security Agenda objectives	20
Table 2:	Reported crimes	105
Table 3:	Law enforcement and related authorities in Sweden	107
Table 4:	Analysed cases	111
Table 5:	Summary of group characteristics	137
Table 6:	Offline groups entering cybercrime	181
Table 7:	Offlineborn groups	182
Table 8:	Cyberborn groups	184
Table 9:	Characteristics of Cyber-OC groups – summary	204
Table 10:	Immaterial damage caused by Cyber-OC groups	209

I. Introduction

The project team

1 Background

Worldwide the digitalisation of society is proceeding rapidly, while influencing almost all areas of life. Especially because of trends like the growing number of networked devices (the ‘internet of things’), citizens’ and societies’ dependence on the internet will continue to grow. Since law-abiding society continuously interacts with digital-based devices and tools that are often connected to the internet, it would be naive to think that the criminal world would act differently. Yearly figures, e.g. from Europol, show that the volume of cybercrime is increasing rapidly. For law enforcement it is challenging to keep up with this modern type of crime. Besides the necessary infrastructure within the prosecution authorities to investigate this complex crime, it also requires highly skilled investigators. In addition, new legal regulations need to be adapted to the ‘digital era’, as the growing use of ICT exposes individuals and all areas of society (e.g. industrial production, administration, healthcare, the electrical power supply) to a huge risk of being targeted by cybercriminals.

The threats arising from different types of cybercrime are real and constantly evolving, as the internet with its anonymity and borderless reach provides new opportunities for physical and virtual criminal activities. We can see complex cybercriminal networks connecting subgroups and also single individuals that are active on, through and against the internet. At the same time there are also ‘offline’ criminal organisations using the internet to facilitate their activities and to increase their profit. Even so-called ‘traditional’ organised crime groups are widening their criminal portfolios by committing cybercrime.¹ By constantly evolving online opportunities, their acts of ‘traditional crimes’ become even more far-reaching and damaging, thus benefiting the criminal organisation.

It is not only the involvement of organised crime in cybercrime that is dangerous, but also cybercrime committed in an organised manner. Cyber-OC represents the convergence of these two phenomena. Despite the huge threat arising from its cumulative character, Cyber-OC is frequently underestimated and differently defined even by law enforcement authorities.

¹ For more details on these insights see e.g.: UNODC, *Comprehensive Study on Cybercrime*, 2013, p. 44; Europol, *The Internet Organised Crime Threat Assessment*, 2014, p. 22; (Interpol: <http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime>).

2 Project objectives and research questions

Owing to the high relevance of the topic for the security of individuals and society as a whole, and because of the lack of relevant empirical research, the central criminological research institutes of Germany, the Netherlands and Sweden – the Criminalistic Institute of the Federal Criminal Police Office (BKA), the Research and Documentation Centre (WODC) of the Dutch Ministry of Security and Justice and the Swedish National Council for Crime Prevention (Brå) – launched a common project. The cooperation between different European countries was necessary and benefited the project because of the inherently transnational nature of the studied phenomenon. The project was funded by the EU programme ‘Prevention of and Fight against Crime (ISEC)’ for the duration of two years (from April 2014 to March 2016).

The project aimed to shed light on the links between cybercrime and organised crime in the three participating countries and on how these two phenomena impact on each other. More precisely, it sought to explore the phenomenon of Cyber-OC by describing its main dimensions such as development context, characteristics of suspects, groups, modus operandi, damage and investigative measures.

This was elaborated on in the different country studies, depending on the available information. For this reason particular aspects were emphasised differently in the three country studies. However, the following research questions represent the common research basis:

- What does ‘Cyber-OC’ mean?
- Do organised crime groups get involved in cybercrime?
 - What sort of (cyber)crimes do they commit?
 - How do organised crime groups use the internet to commit ‘conventional crimes’?
 - What effect does the internet have on the structures of organised crime?
- Is cybercrime organised and how do ‘cybercriminals’ cooperate with each other?
- Does the internet provide new ‘windows of opportunity’ for the development of new business ideas and for the identification of new sources of criminal income?

The necessity to study the linkages between organised crime and cybercrime, instead of investigating the two phenomena separately, was based on several considerations: firstly, the involvement of (traditional) organised crime groups in cybercrime is inherently dangerous, as they not only can build upon a proven structure, conspiracy and effective 'division of labour', but at the same time the use of ICT allows them to expand their impact and earnings. Secondly, cybercrime committed even by single offenders represents a serious crime. When committed in an organised way, perpetrators benefit from broader opportunities, expertise and flexibility, which makes cybercrime even more challenging for law enforcement. Finally, the significance of and threat potential arising from Cyber-OC are still new and often underestimated by politicians, academics and law enforcement authorities. Accordingly, there is a lack of knowledge and law awareness and only little consideration has been given to effective countering.

The project represents an explorative study in which the participating countries conducted research quite flexibly, resorting to some major concerted instruments in order to contribute to a common picture of Cyber-OC. The analyses in the participating countries are designed as case studies that draw on the evaluation of literature, criminal investigation files and expert interviews. Hence the project represents a first-time empirical description of the Cyber-OC phenomenon based on the assessment of its visible characteristics.

3 Definitions

As there is neither a single universal definition of cybercrime nor of organised crime, the project partners agreed upon a common understanding of the two phenomena.

The common basis for the understanding of cybercrime is taken from the 'Convention on Cybercrime', the first international treaty on crimes committed via the internet and other computer networks.²

In respect to the concept of organised crime, the differences between the participating countries were more apparent, as the definitions ranged from a strict organised crime definition used by the police in Germany, to a broader understanding in the Netherlands and Sweden. Because of these different definitions as well as accordingly differing law enforcement countering concepts, each of the three case studies contains a reflection on the term 'organised crime'.

² Council of Europe 2001.

Based on the literature review (see Appendix) the partners developed a common working definition of Cyber-OC, necessary not only for the selection of police files but also for the gathering of data and the subsequent analyses and interpretations.

The working definition of Cyber-OC comprises the Europol definition of organised crime on the one hand (A) and four categories of cybercrime as formulated by David S. Wall and James Martin on the other hand (B). Hence, in order for a case to be considered as relevant for this project, it needed to fulfil Europol's organised crime definition and furthermore to fit into at least one of four cybercrime categories.

(A) Definition of organised criminal groups/networks

For any crime or criminal group to be classified as 'organised crime' at least six of the following characteristics must be present, four of which must be those numbered **(1)**, **(3)**, **(5)**, and **(11)**:

- (1) collaboration of more than two people**
- (2) each with his or her own appointed tasks
- (3) for a prolonged or indefinite period of time**
- (4) using some form of discipline and control
- (5) suspected by the commission of serious criminal offences**
- (6) operating on an international level
- (7) using violence or other means suitable for intimidation
- (8) using commercial or business-like structures
- (9) engaged in money laundering
- (10) exerting influence on politics, the media, public administration, judicial authorities or the economy
- (11) determined by the pursuit of profit and/or power.³**

³ EUROPOL's criteria for organised criminal groups (Doc 6204/2/97 ENFOPOL 35 Rev 2).

(B) Four categories of cybercrime⁴

- (1) **Computer integrity crimes:**⁵ ‘Computer integrity crimes assault the security of network access mechanisms. They include hacking and cracking, vandalism, spying, denial of service, the planting and use of viruses and Trojans.’⁶
- (2) **Computer-assisted crimes:**⁷ ‘Computer-assisted crimes use networked computers to commit crimes, usually to acquire money, goods or services dishonestly. In addition to internet frauds there are socially engineered variants [...] and the manipulation of new online sales environments, particularly auction sites.’⁸ They also include piracy, extortion using ransomware, online prostitution and the use of internet-based tools in relation to human trafficking and money laundering.
- (3) **Computer content crimes:** ‘Computer content crimes are related to the illegal content on networked computer systems and include the trade and distribution of pornographic materials as well as the dissemination of hate crime materials.’⁹
- (4) **Online illicit marketplaces (OIM) / cryptomarkets:** ‘A cryptomarket may be defined as an online forum where goods and services are exchanged between parties who use digital encryption to conceal their identities. [...] The reliance on encryption technology differentiates cryptomarkets from other types of OIM.’¹⁰ Thus, this category includes cases where goods and services are exchanged between offenders on online marketplaces.

As a result of the common definition, certain types of crimes were not included in the study even though they were carried out in organisational structures. For example, hacktivism and (child) pornography are mostly motivated

⁴ The four categories consist of David S. Wall’s three cybercrime types and James Martin’s online illicit marketplaces/cryptomarkets.

⁵ ‘Computer integrity crimes’ or ‘cybercrime in a narrow sense’ = ‘offences against the confidentiality, integrity and availability of computer data and systems’ (Council of Europe 2001).

⁶ Wall 2007, p. 49.

⁷ ‘Computer-assisted crimes’ or ‘cybercrime in a broad sense’ = offences that are committed by means of computer data and systems.

⁸ Wall 2007, p. 50.

⁹ Wall 2007, p. 50.

¹⁰ Martin 2013, p. 6.

by other means than profit and/or power, and were thus excluded from the selection of cases.

Because of different interpretations of group patterns in cybercrime, the researchers agreed to handle the working definition relatively liberally. If a file did not fulfil all the mandatory characteristics, but was deemed to be relevant for the project (by police investigators), it was possible to include it for analysis.¹¹

4 Methodology

The project aims at closing the knowledge gap on the linkages between organised crime and cybercrime. As stated above, the project seeks to explore different forms of criminal organisations in cybercrime in the three countries by highlighting the specific characteristics of the *modi operandi*, structures and offenders' 'profiles' of organised criminal groups and their crime activities on, via and against the internet.

The data was collected in three countries that differ in some aspects of the criminal laws and the countering strategies concerning organised crime and cybercrime. One example of the different legal frameworks within the police authorities is that the Netherlands follows the discretionary prosecution principle, which allows the prosecution service to decide whether to start, continue or stop the investigation of a crime. The public prosecutor determines how investigative resources are deployed and, based upon the results obtained, decides whether or not to prosecute a suspect. When, for instance, resources or time are scarce, the public prosecutor can decide to focus on important facilitators of a criminal organisation instead of the whole organisation. In Germany the law enforcement authorities follow the principle of mandatory prosecution, which obliges the prosecution authorities to take action *ex officio* whenever the suspicion of a criminal offence arises, even if no complaint has been filed. After an investigation has been completed the state prosecutor decides whether to continue with the criminal proceedings. The Swedish system is based on the principle that a crime with a certain de-

¹¹ As an example, one police file in the Dutch analysis does not meet the first criterion – a co-operation of more than two people. In this particular case, the police have been able to identify only one suspect. However, the *modus operandi* in this case was too large for one person to operate and maintain, so it was likely that others were cooperating with this one identified suspect. This fact combined with the benefits the suspect offered as an important facilitator for committing cybercrime gave reason to expect that this particular case was a matter of Cyber-OC. Despite the fact that the case did not meet all the required organised crime criteria of the Europol definition, it provided interesting insights into the *modus operandi*, the police investigation and the high operating level of the cybercriminal.

gree of suspicion must be investigated, and when it is, if the evidence indicates that the prosecutor will reach a conviction, the prosecutor has to go to court. But the possibilities of limiting the investigations are wide and when it comes to organised crime, it is quite common to determine that the investigation and prosecution will cover only certain crimes and perpetrators. Otherwise, the investigations run the risk of being too broad, taking too much time and misusing the resources. Clearly, these different ways of handling the investigations have consequences for the content of the studied files.

In some cases, the Swedish pre-trial investigations do not hold much information about the police investigations, but in other cases, the background material could be substantial. It all depends on how much the police and the prosecutor limit the investigation. A very straightforward investigation will only partly cover the organisational network and its functions. In the Netherlands the studied files were closed police files, which provide a lot of information about the investigative tools and tactics used by the police. In Germany, the studied files were closed police files that had been forwarded to the public prosecutor. As the guiding principle in collecting them was that the crime was committed in an organised way, in all of the cases information on the cooperation between the suspects was included.

A further distinction was the fact that the Swedish categorisation of Cyber-OC groups is based upon ‘crime types’ and on the question of whether they are ‘traditional organised crime’ offences or cyber-specific offences. The German categorisation refers to the groups and classifies them according to the reason for and place of the group formation. By contrast, the Dutch case study did not resort to any form of categorisation. The focus here was placed on the role and skills of the individual suspects within a Cyber-OC group or network.

As a result, the three case studies each have their own focus, making a direct comparison of the findings between the three countries difficult. Nonetheless, the variations in the case studies show that the topic of Cyber-OC is quite extensive and covers a broad spectrum of issues, such as organisational structures, hierarchies and roles. A strong point of our research is the fact that owing to the different emphases of the case studies, the national findings of each individual country can be seen as complementing each other.

Moreover, this is not a representative study of all possible empirical entities, but a first explorative study of this specific phenomenon. Therefore, the findings cannot be generalised. Instead, they should be seen as incipient observations on a deliberate selection of cases that have come to the attention of the law enforcement authorities. Accordingly, our findings cannot be asserted to

hold true for all previous, current and future similar crime or to be transferable one-to-one to other countries or even crime fields. Nevertheless, the study delivers important evidence-based implications on the manifestation of Cyber-OC.

4.1 Literature review¹²

The project started with a literature review aiming to get a comprehensive understanding of the problem area, to understand country specific contexts and to develop a working definition of the concept of Cyber-OC. For this purpose a systematic analysis of published literature, including previous research projects, studies, scientific papers, doctoral and diploma theses, monographies and government reports in English, German, Dutch and Swedish was carried out. This analysis focused on relevant topics including approaches, crime forms, structures and roles as well as profiles of offenders and groups related to cybercrime and organised crime. This review revealed that the topic of organised crime has the attention of researchers, and the same holds for the topic of cybercrime. However, research focusing on the conjunction of the two phenomena appears to be scarce.

The first step for the literature review included a systematic, keyword-based search for relevant open sources. A list of predetermined terms¹³ was used to search online e.g. in library catalogues and on websites of relevant institutions as well as in specific databases containing relevant literature. Moreover, in addition to the keyword research, relevant literature was also identified by a 'snowball system', i. e. sources were recognised through the bibliographies of particularly relevant literature.

The sources focus on the overlap of organised crime and cybercrime and were categorised as: with no reference, with indirect reference and with direct reference. By the end of 2014, 140 publications had been identified as relevant, i. e. having either direct or indirect reference. Because Cyber-OC is getting more and more attention from researchers, while writing this report some recently published relevant papers were also added to the review.

The second step was to systematically summarise the content of the identified literature. This was done by all three partners through a common coding system that comprised a series of questions reflecting the project's research ques-

¹² The literature review is attached in the Appendix of this book.

¹³ These include cybercrime / internet crime / computer crime in combination with organised crime / organised group(s)/network(s) in English, German, Dutch and Swedish.

tions as well as the source's formalities.¹⁴ The identified literature was divided amongst the partners and, by using the common document of pre-set questions, every partner was able to read different sources but still focus on the same subjects, assess the information correspondingly and summarise the content likewise by answering the same questions based on the text.

4.2 Empirical data collection

In order to be able to discuss all the findings at the end of the project, the three case studies were carried out by similar means and with common instruments. At the same time, all three project partners agreed to handle the data gathering and the interpretation of the results according to national context specifics. The targeted research included the analysis of criminal investigation files, expert interviews both with persons specifically involved in the selected and analysed cases and with representatives from police, justice and other relevant authorities and bodies as well as individual expert meetings, seminars and workshops to cross-check the results with invited experts e.g. police investigators, prosecutors, people working with IT security and researchers within the area of cybercrime and/or organised crime. Each of the three project partners was responsible for independently conducting the case studies. The results are presented in the country-specific chapters.

The case studies focus on the gathering and analysis of empirical data based on systematic data collection from police files. For the selection of files the working definition was used, as described above.

For the purpose of the empirical data collection, each partner selected a total of approximately 15 criminal investigations conducted in the corresponding country. The process of identifying and collecting the police files differed among the countries.

In the Netherlands, the police were asked for cases that would contribute to the study of the phenomenon of Cyber-OC, fitting within the definitions as set for this project. Inquiries with an international dimension were of particular interest. A clear preference was expressed for recent case files, given the rapid progress of technological innovation and constant changes in the way cybercrime manifests itself. From a list of all Cyber-OC inquiries, the police and prosecution experts selected those likely to be most valuable to the research project.

¹⁴ The common coding system included, among other things, the following information: author(s), definitions and methods used, characteristics of organised crime groups and networks entering cybercrime, of the organisation of cybercrime, and of perpetrators.

In Sweden, the police work with fixed criminal codes when registering reports (SCB 2011). Of these codes, only seven concern cybercrime: hacking, computer fraud, internet-assisted fraud, (computer) sabotage, internet-related child pornography crime, copyright infringement through file sharing and crimes against industrial property rights with the help of the internet (Brå 2012b). Furthermore, the codes are based on offences but add some characteristics to the crime. Hence, most of the criminal codes register whether the crime was committed indoors or outdoors as well as the victims' sex, age and other details. However, practically no codes show whether the crime occurred over the internet (Brå 2015a). This leads, for example, to a receiving offence committed through a website being registered as 'only' a receiving offence (RPS 2014). In this way, most of the crimes that are cyber-related are not registered as such. In relation to the organised aspects, these codes do not take the number of offenders involved into account and such information is thus not registered. In summation, the consequence of this structure and usage of criminal codes is that Brå was reliant on a snowball collection of data where the researcher identified Cyber-OC cases in accordance with the common definition.

In Germany a twofold approach was used to compile the selected cases, which focused on criminal groups that committed crimes on, through and against the internet on the one hand and on cybercrimes that had been committed by several suspects collaboratively on the other hand. To collect cases, inquiries were made to federal and state authorities, aiming to ensure that all the Cyber-OC investigations carried out in Germany within a certain time frame were documented for the project.

4.3 Common checklist

A common checklist was used as an analytical tool by each partner in order to keep the same focus and, if possible, extract the same type of information from the criminal files. This checklist was composed of different categories, corresponding to the aims of the research project. The common checklist was filled in by the researcher with information gathered from the case files and interviews carried out with the responsible prosecutor or police officers involved in each case. A separate (but identical) checklist was used for every case file analysed. By using this common checklist, all research partners extracted equivalent types of information from their data, which was later to be analysed.¹⁵ The common checklist was an adapted version of the method ori-

¹⁵ The common checklist included, among other things, information on the following codes: 1) suspects/actors, 2) organisation and structure, 3) activities, modi operandi and 4) investigation process.

ginally developed by Kleemans et al. at the end of the nineties to investigate the nature of and the developments in organised crime in the Netherlands (see Kleemans, Van den Berg & Van der Bunt, 1998;¹⁶ Kleemans, Brienen & Van de Bunt 2002;¹⁷ Van de Bunt & Kleemans 2007¹⁸). Specific topics relevant to cybercrime were added to the original checklist. For instance a question was added regarding how people were gaining trust of others in online relations. Another example of an added question was regarding which currency was used when laundering money or paying for goods. Using the checklist resulted in a large pool of qualitative data taken from the selected police files. This data was relevant to answering the research questions.

4.4 Common analysing system

While the previous section described the first step of the data analysis: how the checklist was used to extract relevant information from the police files, this section focuses on the second step: how the information was analysed.

The research partners used qualitative analysing systems (by applying suitable software such as MAXQDA or ATLAS.ti). By basing the analysis process on joint codes, the method of analysing was similar for all project partners. The joint set of codes consists of focus areas and underlying sub-areas, all corresponding with the research aim – to gain knowledge on the characteristics of the modi operandi as well as the structure and offender ‘profiles’ of Cyber-OC groups. The focus areas thus include questions on group background and structure, crime logistics etc. Furthermore, the reason for using the same instruments and sets of codes was to enable the research partners to systematically analyse the different phenomena of the collected data independently of one another but with the same focus.

¹⁶ E.R. Kleemans, E.A.I.M. van den Berg & H.G. van de Bunt, with the cooperation of M. Brouwers, R.F. Kouwenberg & G. Paulides, *Organized crime in the Netherlands: Report based on the WODC-monitor [English summary]*, The Hague, Boom Juridische uitgevers (Onderzoek en beleid 173), 1998.

¹⁷ E.R. Kleemans, M.E.I. Brienen & H.G. van de Bunt, with the cooperation of R.F. Kouwenberg, G. Paulides & J. Barendsen, *Organized crime in the Netherlands: Second report on the organized crime monitor [English summary]*, The Hague, Boom Juridische uitgevers (Onderzoek en beleid 198), 2002.

¹⁸ H.G. van de Bunt & E.R. Kleemans, with the cooperation of C.J. de Poot, R.J. Bokhorst, M. Huikeshoven, R.F. Kouwenberg, M. van Nassou & R. Staring, *Organized crime in the Netherlands: Third report of the organized crime monitor [English summary]*, The Hague, Boom Juridische uitgevers (Onderzoek en beleid 252), 2007.

To sum up, the overall methodological approach includes various methods and refers to both primary and secondary data. In general, the data collection of this project is based on the following four key elements:

- Literature review
- File analysis
- Interviews
- Expert meetings, seminars and workshops

A comprehensive analysis of the state of the art of relevant literature was done as a first step in the project and is attached in the Appendix of this book. This introductory chapter is followed by the three national case studies, which are structured in a similar way: introduction; methods of the national case study containing the specific steps undertaken by each country concerning the case selection process; empirical findings in respect to Cyber-OC suspects, Cyber-OC groups, *modi operandi*, damage, and investigative measures; national case study conclusion. A common presentation of the findings of the three national case studies is included in the last chapter ‘Concluding remarks from the three case studies’.

II. Cyber-OC in the Netherlands

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

In this chapter the results of the research project in the Netherlands are presented. Before we present the results of the Dutch study, the first paragraph will provide a framework of the Dutch procedures, relevant laws and institutions.

1 Organisation of investigation and prosecution in the Netherlands

This paragraph 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 (NCSC), 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.¹⁹ 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.

¹⁹ See Van der Leij, J. B. J. (2014), Het Nederlandse strafrechtssysteem [The Dutch criminal justice system]. In: *Criminaliteit en Rechtshandhaving 2013, Ontwikkelingen en samenhangen* [Crime and law enforcement 2013, developments and cohesion]. WODC, Boom Lemma. ISBN 978-94-6236-511-7; Tak, P. J. P (2008), *The Dutch Criminal System*, 3rd edition. Nijmegen: Wolf Legal Publishers. ISBN 978-90-5850-342-8.

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 level 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 on 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 Art. 10 of the Dutch Code of Criminal Procedure (*Wetboek van Strafvordering*, DCCP), 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 examining magistrate – 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 examining 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 examining judge considers whether their authorisation is reasonable and proportionate, and subsequently checks that the conditions imposed for their use have been complied with.²⁰

1.1 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 was costing the Netherlands at least €8.8 billion a year.²¹ There are also indications that organised crime is becoming more and more involved in cybercrime.²² 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 2014.²³ 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).²⁴ Compared with the staff in other police units, a large part of this team have an IT 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 being left untouched. In order to overcome this, it has been decided to extend investigative capacity in this field to the regional police units.²⁵ 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 larger, more complex cases and cases of national importance. As one member of that team put it in an interview, ‘Today’s

²⁰ Ibid. For more information about the assessment criteria for public prosecutor applications for warrants to intercept communications and their authorisation by an examining judge, see Hoge Raad (Supreme Court of the Netherlands), 11 October 2005, LJN AT 4351.

²¹ <http://www.mcafee.com/us/resources/reports/tp-economic-impact-cybercrime2.pdf>.

²² Van der Hulst & Neve 2008, p. 33.

²³ CotEU 2015, p. 21; *Wervingsfolder Politie* [Police recruitment brochure] 2013, p. 5.

²⁴ CBA 2012, p. 12.

²⁵ *Veiligheidsmonitor* [Security Monitor] 2015–2018.

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 covered by the regional police. That is not to say that 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 such as 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 specifically to improve the police's ability to fight cybercrime at the regional level.²⁶ Under the 2014 Tactical Programme for High-Tech Crime, the NHTCU is required to reserve 40 per cent of its investigative capacity for handling requests for assistance from other agencies and for incident-led inquiries. The remaining 60 per cent is devoted to the team's so-called priority areas: cyberattacks on vital infrastructure and the financial system and investigations into ransomware, facilitators and botnets.²⁷

This increased focus on 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.²⁸ 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.²⁹

²⁶ CotEU 2015, p. 20.

²⁷ *Tactische Programma High Tech Crime* [Tactical Programme for High-Tech Crime] 2014, p. 20.

²⁸ *Veiligheidsmonitor* [Security Monitor] 2015–2018, p. 5.

²⁹ *Ibid.*

Table 1: Public Security Agenda objectives

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

Source: Public Security Agenda 2015-2018

‘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 the 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 expertise in this field and do not prioritise these cases. As one of the respondents told the researchers, ‘Blood comes before bytes.’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 in 2016 and rising permanently to €2.7 million a year from 2017 onwards.³¹

National Cybersecurity 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 re-

³⁰ Struiksma, De Vey Mestdagh & Winter 2012, p. 30; <http://www.politieenwetenschap.nl/cache-/files/55f6cc2b539f1Cybercrime.pdf>.

³¹ *OM Meerjarenplan Cybercrime* [Public Prosecution Service Long-Term Plan for Cybercrime] 2015–2018, p. 4.

leased 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 cybersecurity.³²

‘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.’³³

This policy vision has been translated into an NCSS Action Programme for 2014–2016,³⁴ 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:³⁵

- 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 cooperation 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.³⁶ 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

³² NCSS 2, p. 17: https://www.nctv.nl/Images/ncss-2-webversie-def_tcm126-519975.pdf.

³³ NCSS 2, p. 7: https://www.nctv.nl/Images/ncss-2-webversie-def_tcm126-519975.pdf.

³⁴ Ibid, p. 27 (Appendix 1).

³⁵ *Veiligheidsmonitor* [Security Monitor] 2015–2018; CotEU 2015, p. 13; NCSS 2, pp. 27 et seq.

³⁶ CBA 2012, p. 10.

these crimes can now be reported on the main police website. However, there is still a special site to report online child pornography.

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, such as banks, with relatively well-protected IT systems.³⁷ 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 2011.³⁸

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 Cybersecurity Centre

The National Cybersecurity 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,³⁹ 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 co-ordinating role in the event of an IT crisis. It also updates the public and SMEs (small and medium-sized enterprises) on the safe use of the internet by providing general information and specific current warnings

³⁷ CBA 2012, p. 13.

³⁸ ECTF Covenant: <https://www.rijksoverheid.nl/documenten/convenanten/2011/03-15/convenant-samenwerking-en-informatie-uitwisseling-electronic-crimes-task-force>; interview with ECTF.

³⁹ <https://www.ncsc.nl/organisatie>.

through the website www.veiliginternetten.nl, thus enhancing wider awareness of cybersecurity issues. From the literature, however, it is apparent that the centre is still searching for its precise role. The NHTCU and the Public Prosecutor Service consult regularly on this matter.⁴⁰

1.2 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’. 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, 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 Art. 80sexies of the DCC as ‘a single device or group of combined devices that automatically processes and transfers data’. This is a broad definition that 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 a broad sense means ‘traditional’ offences carried out with the aid of computers and the internet. In these cases computers and the internet are used as significant tools for crime. This often brings an international di-

⁴⁰ *Tactisch Programma High Tech Crime* [Tactical Programme for High-Tech Crime] 2014, p. 8.

mension to the criminal act. Online fraud, webshop swindles and electronic money laundering are examples of this ‘broad’ category of cybercrime.⁴¹

History of the Dutch legislation

Over the years, the Dutch Criminal Code (DCC) and Dutch Code of Criminal Procedure (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.⁴² 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.⁴³ Amongst the activities rendered unlawful under CC I were hacking, spreading viruses, wilfully corrupting data, intercepting data traffic without authorisation and forging bank cards.⁴⁴ 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. Previously, such orders could not have been issued because no suspect could be forced to cooperate in their own incrimination by, for instance, revealing access codes.⁴⁵

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 tackle this form of criminality at the international level.

⁴¹ Kaspersen 2004; CBA 2012, p. 11.

⁴² Koops 2007, p. 19; Kaspersen 1990.

⁴³ Koops 2012, p. 13; Koops 2010, p. 3.

⁴⁴ See DCC Art. 138ab, 138b, 350a and 350b, in conjunction with Art. 80.

⁴⁵ See Art. 125i-o DCC

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 Art. 126 DCCP, which requires the examining magistrate to set clear investigative parameters.⁴⁶

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.⁴⁷ Although alternatives have been discussed, as yet the parties to the Convention have failed to find a way to enhance international cooperative arrangements in this respect.⁴⁸ 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. As Koops and Goodwin aptly point out, 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.⁴⁹

The Netherlands signed the Convention on Cybercrime on 23 November 2001 and it was ratified by the government on 16 November 2006. As of 2015, it has been signed and ratified by a total of 46 states.⁵⁰ Besides most of the members of the Council of Europe, they include important nations such

⁴⁶ Stol et al. 2012, pp. 29–30.

⁴⁷ Kaspersen 2006, p. 21.

⁴⁸ *Convention on Cybercrime*, par. 193. <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CL=ENG>.

⁴⁹ Koops & Goodwin (2014), *Cyberspace, the cloud, and cross-border criminal investigation*. The Hague: WODC.

⁵⁰ <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CL=ENG>.

as the United States, Canada, Japan and South Africa.⁵¹ According to the official chart of signatures and ratifications, however, the Netherlands is one of relatively few countries to have implemented the Convention at the national level.⁵²

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 Art. 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 Art. 138ab DCC focuses on the intent underlying an intrusion and less on whether or not hackers know that their actions are unlawful.⁵³ Other new measures included criminalising denial-of-service (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,⁵⁴ in a manner that often raises jurisdictional questions. The principal applied in the Netherlands is that of ‘computer-based jurisdiction’, with the physical location of the server, or other ‘computerised device or system’, determining which jurisdiction is applicable.⁵⁵ In effect, this means that law enforcement agencies cannot do anything if the server is outside the Netherlands.⁵⁶ 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,

⁵¹ Kaspersen 2004.

⁵² <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CL=ENG>.

⁵³ 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.

⁵⁴ Koops 2012, p. 9.

⁵⁵ Klip 2000, p. 140.

⁵⁶ Art. 125j DCCP. On extraterritorial searches, in principle not permitted, see Wiemans (2004), *Onderzoek van gegevens in geautomatiseerde werken* [Investigating data in computerised devices and systems], pp. 152–162.

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.⁵⁷ 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. 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 is more, following the advice given by the Council of State,⁵⁸ the new draft will have stricter privacy guarantees. Consequently, the bill has been adjusted and improved 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 ‘counter-hack’, 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.⁵⁹ Below we describe the proposed new powers in more detail in order to provide a first impression of what the government hopes to achieve by introducing them.

⁵⁷ *Kamerstukken II* [Dutch parliamentary document] 2004/05, 26 671, no. 10, p. 23.

⁵⁸ *Kamerstukken II* [Dutch parliamentary document] 2015/16, 34 372, no. 4.

⁵⁹ See also: Koops & Goodwin (2014). *Cyberspace, the cloud, and cross-border criminal investigation*. The Hague: WODC.

The power to intrude into a suspect's computer – 'counter-hacking' in popular parlance – is described in the proposed Art. 126nba DCCP. This would allow investigators to monitor a suspect's activities prior to the encryption of data. Having counter-hacked a device, police would be authorised to carry out numerous operations, from establishing the suspect's identity to extracting data and observing it systematically. With the increasing use of cloud computing and servers abroad, transnational investigation is already a thorny issue and its potential extension to include extraterritorial counter-hacking powers is highly controversial. Therefore, such hacks would only be permitted if they were in the 'urgent interests' of an investigation and with a warrant issued by the Public Prosecution Service and endorsed by the examining magistrate. 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.⁶⁰ This paragraph has been added to the article in the draft. There are, however, exceptions to be made when there are social and economic interests at stake. One might think of a DDoS attack on a bank or the situation of 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 Art. 125p DCCP, which complements the existing Art. 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 worth of internet fraud claims in 2014.⁶¹ This new bill therefore proposes that the repeated offering of goods and services without actu-

⁶⁰ Art. 126nba(1c) DCCP.

⁶¹ *Kamerstukken II* [Dutch parliamentary document] 2015/16, 34 372, no. 3, p. 72.

ally delivering them will also become a criminal offence. It is suggested to make this crime punishable by a four-year 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 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 2000,⁶² 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) information gathering, (5) clandestine entry, (6) electronic interception of communications and (7) remote monitoring of communications.⁶³

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 Art. 67,

⁶² For an extensive description, see, for example: 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 BOB: Books IVa and V in practice, decisions on special investigative powers to combat organised crime], Uitgeverij Boom.

⁶³ Beijer et al. 2004, p. 277.

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 examining 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 examining judge's consent.

The examining 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 examining 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' – better known as 'counter-hacking'. In a memorandum to Parliament, the Minister of Security and Justice has stated that such searches are permissible, subject to authorisation by an examining judge, under Art. 125i DCCP.⁶⁴ In practice, though, it seems that they are carried out only occasionally.⁶⁵ What is more, there is no literature that suggests the DCCP provides a legal justification for hacking as an investigative power.⁶⁶

⁶⁴ *Kamerstukken II* [Dutch parliamentary papers] 2014–2015, 286. <https://zoek.officielebekendmakingen.nl/kv-tk-2014Z14361.html>.

⁶⁵ See *Rechtbank Rotterdam* (Rotterdam District Court), 26 March 2010, LJN BM2520, and *Hof 's-Gravenhage* [The Hague High Court], 27 April 2011, LJN BR6836.

⁶⁶ Koops & Buruma 2007, p. 118 in: Koops 2007 (Koops, E.J. & Buruma, Y. (2007), 'Formeel strafrecht en ICT', in: Koops, E.J. (ed.) (2007), *Strafrecht & ICT*, Monografieën Recht en Informatietechnologie, no. 1, 2nd edition. The Hague: Sdu Uitgevers).

Nonetheless, special investigative powers – in both their online and their off-line variants – play a major part in the detection of cybercrime. Under Art. 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,⁶⁷ 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.⁶⁸ 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 2013.⁶⁹ 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 2014.⁷⁰ In any case, intercepting voice communications can be just as useful in the investigation of cybercrime as tracking internet traffic. The same is true of 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.⁷¹ 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 tele-

⁶⁷ 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 Use of Telephone and Internet Taps in Criminal Investigation], *Onderzoek en Beleid* 304. The Hague: Boom Lemma, p. 12.

⁶⁸ *Kamerstukken II* [Dutch parliamentary papers] 2013–2014, 33 930 VI, no. 1, p. 50.

⁶⁹ *Ibid.*

⁷⁰ *Kamerstukken II* [Dutch parliamentary papers] 2013–2014, 33 930 VI, no. 1, Appendix, p. 17.

⁷¹ Odinot, G., Jong, D. de, Bokhorst, R. J., & Poot, C. de (2013), *The Dutch Implementation of the Data Retention Directive*. The Hague: WODC/Boom Lemma, https://www.wodc.nl/-/images/ob310-summary_tcm44-534135.pdf.

phones. 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 this made a very valuable contribution to detective work.

The European directive has always been controversial, and was not well-received in all member states. Critics claimed that it excessively infringed on personal privacy and was 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.⁷² 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.

As a result, telecommunications providers no longer have to retain data for a set period. The Public Prosecution Service⁷³ 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.⁷⁴ Even the civil court that annulled the law stated that scrapping the data retention ‘could have far-reaching consequences for the investigation and prosecution of criminal acts’.⁷⁵ The Council for the Judiciary too, in a legislative recommendation issued in February 2015, stressed the importance of such a requirement⁷⁶ 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 examining magistrate.⁷⁷ 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

⁷² <http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054nl.pdf>.

⁷³ Ferdinandusse, W. N., Laheij, D., & Hendriks, J. C. (2015), *De bewaarplicht telecomgegevens en de opsporing: Het belang van historische telecommunicatie gegevens voor de opsporing* [Telecoms Data Retention and Criminal Investigation: The importance of historical telecommunications data in solving crime]; https://www.om.nl/public/pages/44621/-de_bewaarplicht_telecomgegevens_en_de_opsporing.pdf.

⁷⁴ Ferdinandusse, Laheij & Hendriks 2015, p. 41.

⁷⁵ Rechtbank Den Haag (The Hague District Court), 11 March 2015, ECLI:NL:RBDHA:2015:2498, r.o. 3.12.

⁷⁶ Letter from the RvDR, 2015.

⁷⁷ Ibid.

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.

2 Methodology

In order to gain insight into offenders, cooperating structures, organised criminal groups and their *modi operandi* on, via and against the internet and into the implications of the internet for law enforcement, 11 criminal investigations were analysed.

2.1 Selection of Dutch cases

At the start of this project it was decided, in conjunction with the partners, to conduct research on Cyber-OC by collecting and analysing police case files, according to the methodology as used in the Dutch National Organised Crime Monitor.⁷⁸

In order to gain access to relevant files, we contacted the National Cyber-crime Prosecutor and the police's High-Tech Crime Team. They were very helpful in selecting and making the cases available, so they could be studied and analysed for this project.

From a list of all organised cybercrime inquiries, the police and prosecution experts indicated those likely to be of most interest for this research project. Because we wanted to gather data about as many aspects of the phenomenon as possible, we asked them to choose the 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 cybercrimes in the broad sense and the narrow sense of

⁷⁸ Kruisbergen, E. W., Bunt, H. G. van de, & Kleemans, E. R. (2012). *Georganiseerde criminaliteit in Nederland: Vierde rapportage op basis van de Monitor Georganiseerde Criminaliteit* [Organised Crime in the Netherlands: Fourth report based upon the Organised Crime Monitor], *Onderzoek en beleid* 306. The Hague: WODC.

the term. Nothing was agreed in advance about the proportion of cases falling into each of these two categories, since that might have hindered the search for files and because, ultimately, each research partner has a limited view on the available cases. However, inquiries with an international dimension were of particular interest to us owing to the subject and nature of this study.

We also expressed a clear preference for recent case files, given that technological change and innovation is constantly changing the way cybercrime manifests itself. Thanks to good contacts with the NHTCU, the final selection of cases for the Dutch study was completed without any problems – although, as it turned out, there was not a very large pool to choose from. In the Netherlands the number of completed investigations of organised cybercrime that met the criteria for this research project is limited.

In the end, we selected a total of 11 cases in which the police inquiries have been completed. According to the experts, these collectively provide a good reflection of police and judicial cybercrime investigations during our chosen period. A number have already been tried and judged, but several are still before the courts. Two of the cases were initiated in 2009, one in 2010, three in 2012, four in 2013 and one in 2014. The 11 files examined describe a total of 107 suspects.

We thus chose to investigate cases that provide insight into the various forms of Cyber-OC encountered in the Netherlands, rather than studying a random sample of all such cases.

2.2 Information available in police files

For the Dutch part of the study, police files were examined that describe the alleged facts, provide information about the suspect, the police investigation and the methods used, and also contain witness statements and transcripts of police interviews. As well as revealing details of suspects and their *modus operandi*, the files contain information about ways of cooperation based on, for instance, tapped communication and observations.⁷⁹

2.3 Interviews with experts

Besides the police files we used interviews with 12 law enforcement officials to gather information about Cyber-OC. In order to study each of the selected inquiries and obtain background material, we contacted the public prosecu-

⁷⁹ Ibid.

tors or investigating teams responsible. 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 which case the interviews focused on answering our unanswered questions. With more complex cases, however, before looking at the file in any detail a semi-structured interview was conducted with either the relevant public prosecutor or (in one instance) the secretary at the Public Prosecutor Service overseeing the full inquiry. This was done in order to get an impression of the characteristics of the case. Certainly with large and wide-ranging investigations that have produced large case files, this approach was necessary so as 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 putting further 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 and Europol in tackling Cyber-OC in the Netherlands, so representatives of these organisations were contacted as well. This resulted in a number of interviews, with a total of 12 persons.

3 General description of the Dutch sample

The conducted investigations

The Dutch dataset comprises 11 analysed Cyber-OC case files. Of the 11 inquiries in our sample, ten cases were all handled by the NHTCU. Three were entirely domestic 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 a district level. This was a case in which webshops 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 cooperation with foreign law enforcement agencies.

The fact that only one of the selected cases was dealt with at a district level is a consequence of the focus of this study: Cyber-OC. The ‘organised’ aspect makes these larger and more complex criminal conspiracies, which need to be tackled at a higher 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 11 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 totalling approximately €1 million was withdrawn all over the world. The case file names 12 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: An organised 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 its background, the motives behind it and the suspects are strongly 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 that 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 email 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 pretences 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.

4 Empirical findings

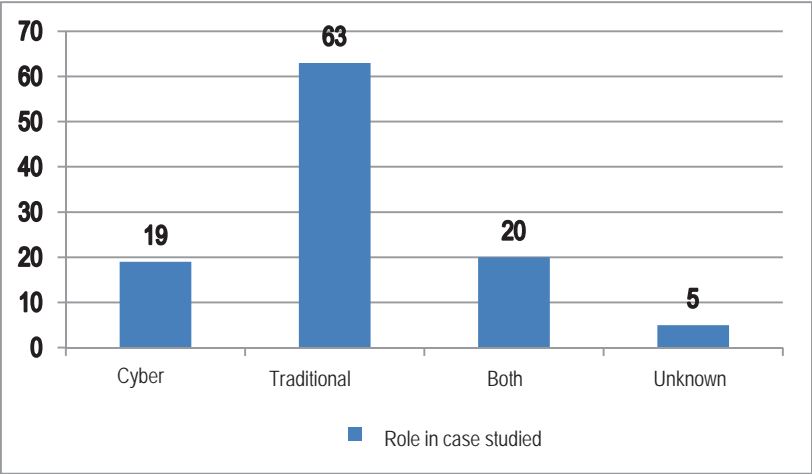
4.1 Suspect characteristics

Suspects in the 11 cases

Overall, 107 suspects are described in the 11 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 investigations into cybercrime, but their own activities were not particularly ICT-orientated.

In terms of background, the suspects are a highly diverse group. Some are university educated, some are 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



Source: 11 analysed police files of the Dutch police

Age

As pointed out earlier in this book, many people think of the ‘typical’ cyber-criminal as young and technically skilled. According to the Deputy Head of the UK’s National Cyber Crime Unit, quoted on the website dutchcowboys.nl,⁸⁰ criminals often try to recruit youngsters with IT skills for illegal activities through online forums and discussion boards.

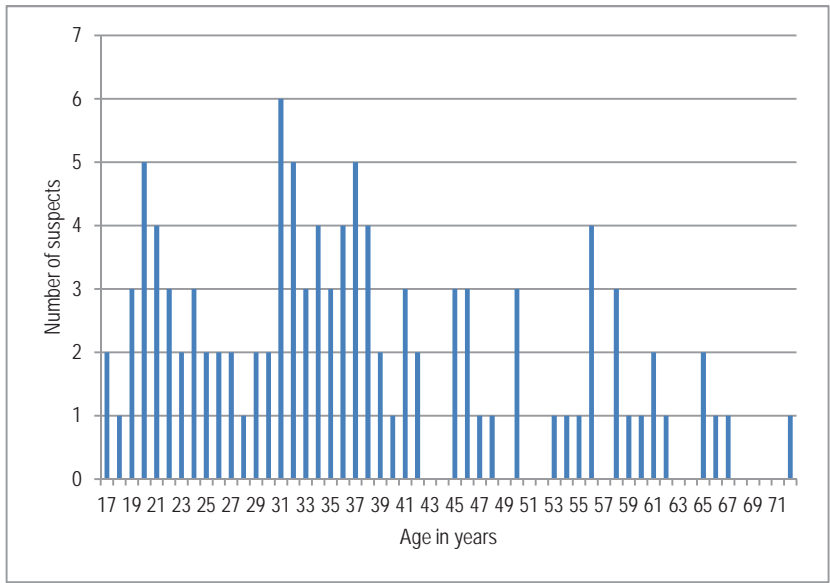
‘More and more teenagers are becoming wired in to a digital environment from an early age, acquiring potentially dangerous skills such as coding and hacking. Technology chat rooms and posting boards are the perfect place for criminals to scout the next generation of highly skilled teens. We need to bear 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 on 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.

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 relate to ICT-orientated crime were slightly younger, averaging 29 years.

⁸⁰ Source: <http://www.dutchcowboys.nl/cybercrime/politie-en-cybercriminelen-zijn-op-zoek-naar-medewerkers-met-dezelfde-vaardigheden>; accessed July 2015.

Figure 2: Suspects by age



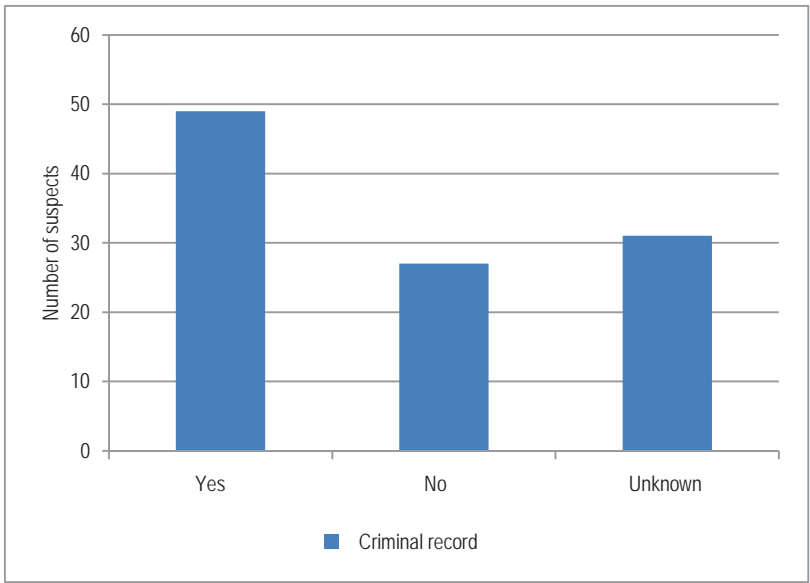
Source: 11 analysed police files of the Dutch police

4.1.1 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 the police. As explained earlier, within the cases studied 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.

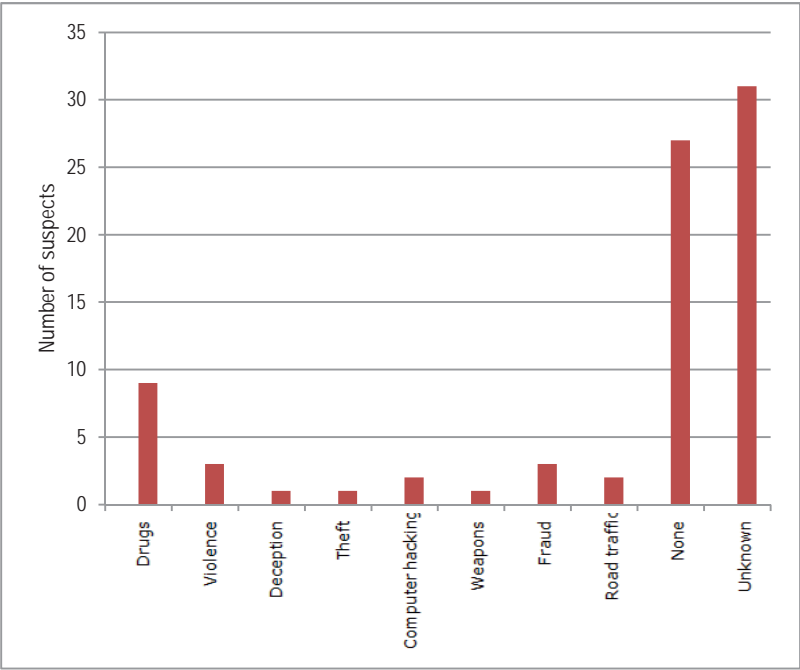
Of the ‘pure’ cybercrime suspects, only three had previous convictions for computer-related offences but six had records for other criminal acts, such as burglary, theft or drug crimes. Eight had no criminal history, and in two instances the criminal history could not be ascertained from the case files.

Figure 3: Suspects with criminal history



Source: 11 analysed police files of the Dutch police

Figure 4: Criminal history of suspects



Source: 11 analysed police files of the Dutch police

4.1.2 Motives

In order to understand and address Cyber-OC 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 bot-nets 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 large debts already existing. 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 cyber-crime. 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 that 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 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 Neve⁸¹ (2008: 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 (Hulst and Neve 2008: 22). Europol (2003: 73 in Van der Hulst and Neve, 2008: 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 (see also NHTCC 2006b: 7)
- 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.

⁸¹ Van der Hulst, R., & Neve, R. (2008), *High-tech crime, soorten criminaliteit en hun daders. Een literatuurinventarisatie* [High-tech crime, different crime types and perpetrators: A literature review], *Onderzoek en beleid* series. The Hague: WODC/Boom Lemma.

4.2 Activities and modi operandi in the field of Cyber-OC

4.2.1 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 emails, 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. Independent research revealed that TorRAT had been developed by the criminal organisation itself⁸² 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.

⁸² <http://computerworld.nl/beveiliging/79823-torrat-bende-anoniem-door-gebruik-vpn-en-bit-coins>.

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 program 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 advantage 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 that involved hacks of a law firm and other targets. The two suspects achieved this by sending out phishing emails 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 that 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 a 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 suspect 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 emails have improved on many different levels. Currently, it proves to be difficult for consumers to distinguish a phishing email from a legitimate email message. It often takes the form of a fake email 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. Phishing can thus be categorised as using the computer as a *tool*.

In one of the cases we see an example of phishing. Using email 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 email installed malware on the victim’s computer.

Another case also used fraudulent emails, apparently from a major Dutch online retailer. In this case, the emails contained a link to a fake version of the webshop, through which unwitting victims supplied the suspects with their login 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 were 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.

4.2.2 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 never 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 strings, such as 'a1987634tormail.org'. Several of the suspects in our cases had dozens of pseudonyms, each with its own email addresses. Their online contacts often focus upon the exchange of information. In one case file, for example, we read of how suspects worked together under aliases on

preparations for a DDoS attack. The exchanges take place in chat rooms, 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 the person's 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 physical 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 email.

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 that 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 to 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 emails are never traced by the 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 own identity.

Protecting communications

Whenever people work together, they need to communicate in order to manage their activities and coordinate 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, 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 their communications were intercepted by police.

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. Research⁸³ 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 studied 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 that 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 an intercepted conversation.

As well as 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.

⁸³ Odinet, G., Jong, D. de, Leij, J. B. J. van der, Poot, C. J. de, & Straalen, E.K. (2012) *Het gebruik van de telefoon- en internettap in de opsporing*. O&B 304. Den Haag: Boom Juridische uitgevers. ISBN 978-90-5931-846-5.

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 15 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 email 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 that 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 this is frequently inaccessible because it is

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 a police infiltrator, 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. Besides 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, the police often need his (or her) cooperation as they can only access his secure data if he is willing to disclose his login 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 cooperated 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 Hot-mail 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 log supplied by a witness, technical analyses and data found on the computer of another suspect.

4.3 Collaboration and organisation

One of the core questions addressed by this study concerns the extent to which cybercrime is organised and how its perpetrators collaborate. That is the topic of this section.

4.3.1 Size and composition of criminal groups

All but one of the 11 cases we studied definitely involved some form of collaboration between suspects. The number of suspects in these ten cases ranged from two to 49. In four instances there were two or three suspects and in another four there were between six and nine, whilst the two largest cases had 12 and 49 suspects respectively.⁸⁴ However, the number of persons of interest in a criminal investigation says more about the focus of the police inquiry than it does about the scale of the cybercrimes committed. As an example, the case with just one suspect 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 one: 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, there are usually some individuals who concentrate on the ICT aspects of the operation and others who focus on other matters. These can range from commissioning a hack to more secondary roles such as 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.

⁸⁴ 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.

4.3.2 Origins of criminal alliances

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, Van der Berg, Van de Bunt 1998; Kleemans et al. 2002: 3), social relationships such as family links and friendships are an important factor in criminal alliances. Kleemans et al. (2002: 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: 3).

In their status assessments of high-tech crime, the police point out some striking differences between Cyber-OC and its ‘regular’ counterpart (CBA 2012: 89). For example, there is usually no physical contact between ‘partners in crime’, only online communication, according to this police report.⁸⁵ 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 deter-

⁸⁵ Leukfeldt (2014) in his article on a phishing case in Amsterdam found that the offenders’ network consisted of real-world social relationships. This is contrary to other research, which often finds that contacts originated from internet forums.

mine 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 chat room, 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 sources of illegal activity. 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 their 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)⁸⁶ also emphasises 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.

4.3.3 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, but may be expedited by a factor such as a common language. 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.

⁸⁶ Leukfeldt (2015), Organised Cybercrime and Social Opportunity Structures: a Proposal for Future Research Directions, *The European Review of Organised Crime*, 2(2), pp. 91–103.

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’.

4.3.4 Facilitation by individuals and companies

As well as the actual suspects, the police files also reveal details of other individuals and companies that 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 that 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 such as 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 such as webshops, courier firms and telecommunications companies, that are exploited by suspects in the perpetration of their crimes – and are sometimes also victims of this. 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.

4.3.5 Organised crime and cybercrime

The research questions posed for this study concern the extent to which organised crime groups use the internet to commit conventional crime and to what extent the internet has given rise to new forms of organised crime.

Based upon the Dutch cases studied, we can say that groups in the Netherlands are involved in cybercrime in three ways. Firstly, there is 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 2005/15: 81-82).⁸⁷ One group, for example, set 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. According to Wall, this is called computer-enabled crime (ibid.). 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 bank cards at cash machines across Europe.

⁸⁷ Wall, D.S. (2005/15). The Internet as a conduit for criminals, pp. 77-98, in: Pattavina, A. (ed.) *Information Technology and the Criminal Justice System*. Thousand Oaks, CA: Sage.

Finally there are the new ‘groups’ developing specifically internet-led criminal activities, also known as cybercrime in a narrow sense or, as Wall calls these entirely new types of crimes, computer-dependent crime or ‘true cyber-crime’ (ibid.). 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 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 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. There are cases, though, 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 this new criminal world, there are sometimes power struggles. These are fought out using weapons such as DDoS attacks.

4.4 Damage of Cyber-OC

A central point in the current policy on the damage and harm of organised crime is so-called ‘undermining’, meaning the intertwining of the legal and illegal structures in society.⁸⁸ In this paragraph we discuss the damage of Cyber-OC. Targets of Cyber-OC can be computers, individuals, companies and authorities. The damage caused by Cyber-OC is material as well as immaterial.

In our cases a first type of damage is financial loss. In several cases hundreds of random civilians were the target of some kind of banking fraud, where their bank accounts or credit cards were used to steal their money. Because these victims are compensated by their banks, these financial losses are for the banks. Also webshops suffered from financial losses in several cases be-

⁸⁸ TK 2015–2016, 29911 no. 120

cause of fraudulent credit card orders. Goods were ordered using the victims' names or their credit card details. Besides direct financial losses, targeted companies incur costs for the investigation of frauds or improvements. Besides money, we see that sensitive information was 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 that owns the website. Reputational damage can also be caused by the use of the National Police logo in emails containing ransomware.

A third type of damage that we encounter in our cases is distrust. Several kinds of cybercrimes cause banks to fear distrust by the general public regarding online banking, e-commerce, and their own good name.

4.5 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 Team. 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 do not yet possess that kind of knowledge.

In this paragraph we examine the investigative methods used and, as far as possible, the reasoning behind those choices.

4.5.1 How cases come to the attention of law enforcement

In none of the case files was 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 such as 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 11 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. Webshops, 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 email. 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 the 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 webshops.

Another trigger is information from abroad. This initiated the Dutch investigation in three of our 11 inquiries. In one case, the source was Europol. Material that 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 that 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 Art. 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 the 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 was a growing problem across Europe, with devices infected in the same way and the logos of local law enforcement agencies often used as part of the deception. Victims also see on-screen 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 searched 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 were 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 none of the case files studied did we find any information originating from the Criminal Intelligence Unit. This is a police squad charged primarily with clandestine information-gathering in support of the investigation of serious and organised crime. Much of the intelligence information from this squad comes from the criminal community itself. It is remarkable that this squad seems to have a limited information position when 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 its internet counterpart as a ‘challenge’ for the future.

4.5.2 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 Cyber-OC – 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 the 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 email 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 an extended 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 ‘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 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 the registered user of a domain name is, 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 an 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 Art. 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.

Telephone and internet taps

At least one telephone tap was used in seven of the 11 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 the police to deploy a surveillance team.

IP taps were also used in seven of our 11 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 to 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 the 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 as to 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 login 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. Criminals 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, emails 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 exam-

ined, or after their user names and passwords were obtained. In one case, a witness gave police his archive of communications logs with a suspect.

Because most internet service providers are based outside the Netherlands, they are not subject to the requirement under Dutch law (Art. 13 of the Telecommunications Act) to allow duly authorised interception of traffic 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 1.2 above) was still in force when our cases were under investigation by 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 emails and IP addresses of visited websites or search terms entered into search engines cannot be requested based on the Data Retention Act.

In all 11 cases, the requested traffic data was 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 11 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 per cent 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.⁸⁹ 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.⁹⁰ This makes it all the more striking that we find both in the 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 infiltrator and in another a listening device installed in a car.

In the former, a Dutch vendor was offering weapons and drugs for sale on 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 physical meeting between the police infiltrator 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.

⁸⁹ 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 use of telephone and internet taps in criminal investigations], *Onderzoek en beleid* 304; The Hague: Boom Juridische Uitgevers.

⁹⁰ *Ibid.*, p. 177. See also Kruisbergen, E. W., & Jong, D. de, with Kouwenberg, R. F. (contrib.) (2010). *Opsporen onder dekmantel* [Undercover investigation], *Onderzoek en beleid* 282. The Hague: Boom Juridische Uitgevers, pp. 136–37.

Another case showed the police gaining access to a server operated by criminals, in order to search it. This was necessary to understand the illegally built system and to learn how it was operating.⁹¹ However, remotely accessing a computer is controversial because one could say the police are ‘hacking’ as well. Moreover, this method is currently not regulated by law, but has been suggested as a new investigative power in the new Computer Crime Bill (see 4.1 above). Once this law is enacted, there will be a legal framework for ‘counter-hacking’.

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 organisation. The police try to get an impression of the individuals of the criminal organisation, 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 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 refused any further collaboration and invoked 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.

⁹¹ For a detailed description, see: Graaf, D. de, Sosha, A.F., Gladyshev, P. (2013) Bredolab: Shopping in the cybercrime underworld, in: Rogers, M., & Seigfriedd-Spellar, K. C. (eds.), *Digital Forensics and Cybercrime*. Fourth International Conference ICDF2C 2013 (pp. 302–313). Racine, WA: Springer. [Ulir.ul.ie/handle/10344/2896](http://ulir.ul.ie/handle/10344/2896).

Sometimes suspects give a reason for their refusal to talk. One suspect, the administrator and head figure in the criminal organisation, said he was too scared to testify. He was threatened; ‘Silence is gold, talking is dead’.

On a rare occasion some suspects testified 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 as to 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.

In the files, the researchers 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 organisation. He wrote that he should have known better and that he regretted his involvement in the organisation. His letter gives a rare insight into how this person reflects on his help to the criminal organisation:

‘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.’

4.5.3 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.

4.5.4 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. Anonymisation software is mentioned on a number of occasions as a way of emailing, 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 such as 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 that 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 email 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, email addresses and the name of a tiny village somewhere far away. This was despite the suspects using Tor and emailing 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 closely known associate was the person behind a given nickname. This is despite the fact that 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.

4.5.5 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 cooperation 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, whom the police had had their eye on, 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 the 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 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. The Dutch police cannot demand material directly from organisations outside their jurisdiction, so the requests are channelled through the appropriate authorities abroad.

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 that 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 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 such as 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 Europol 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 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 had claimed victims across Europe, both Europol and Eurojust were enlisted in an attempt to instigate international cooperation. 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, cooperation 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 ongoing 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.

4.5.6 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',⁹² 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.⁹³

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 deprivation-driven thinking yet penetrated all levels of the police organisation'.⁹⁴ In 2012 the Inspectorate of Public Order and Security ob-

⁹² Nelen, H. (2004), 'Hit them where it hurts most? The proceeds-of-crime approach in the Netherlands.' *Crime, Law and Social Change* 41(5), pp. 517–534.

⁹³ Kruisbergen, Bunt & Kleemans (2012), p. 229.

⁹⁴ Nelen, J. M., & Sabee, V. (1998), *Het vermogen te ondernemen: Evaluatie van de ontneemingswetgeving – Eindrapport* [The capital for business: an evaluation of the criminal confiscation legislation – final report]. The Hague: WODC, pp. 112–13.

served that financial investigation had still not been sufficiently integrated into the work of the police.⁹⁵

This is reflected in the files we studied. In only one case was there 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 to 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 safeguarded. 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 bank cards. 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,⁹⁶ but the file does not mention 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

⁹⁵ Inspectie Openbare Orde en Veiligheid (Inspectorate of Public Order and Security, 2012), *Follow the money!* The Hague: IOOV, p. 10.

⁹⁶ <http://www.bbc.com/news/technology-18189987>, http://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/>.

upon finding evidence of the crime itself rather than its proceeds. On other occasions, the 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 from cash withdrawals around the world after skimming bank cards, but the main suspect 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 their 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 is the stolen amount 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, email intercepts allow us to track an exchange of money into a virtual currency through Western Union. 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 that 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 such as 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 such as Paymer, PerfectMoney and bitcoins, but also to providers of technical solutions such as 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 in cash at his former home.

Convictions

At the time of writing (January 2016) seven of the eleven studied cases have been brought before the court. Of these cases most suspects were sentenced to prison, community service or a fine. In one case the suspects appealed, which led to acquittal for two suspects. An interesting fact is that almost all cases involve foreign suspects, who have also been convicted in the Netherlands in these cases. Finally, there are two cases that have not yet gone to court and there are three cases of which the status is currently unknown.

4.5.7 Challenges, bottlenecks, experiences and best practices

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 High Tech Crime Team, has grown rapidly during recent years. This means there is capacity and expertise reserved especially for cybercrime cases. This dedicated team only focuses on high-tech cybercrime and the criminal investigations of these cases do not have to compete with other kinds of serious crimes. The evidence and information about possible cybercrimes that come to the attention of the police are, however, significant, and even the capacity of the NHTCU is limited. To

interpret our results, it is important to realise that in the Netherlands, owing to the principle of prosecutorial discretion (opportunity principle), public prosecutors have the unrestrained freedom not to prosecute or to drop criminal cases if the prosecution seems in vain. As a consequence, the Dutch police and the Public Prosecution Service can make a selection between cases or suspects and can decide to focus on suspects who are within the reach of law enforcement owing to their location or available information.

From the studied case files and interviews, it becomes clear that investigating cyber (organised) crime can be compared to a complex puzzle that requires different types of expertise.

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, however, appears to have been effective in revealing people's identity in some of the studied cases. These investigative powers can be applied both online and offline. A nice example, found in the files, was an undercover agent acting online to make contact with a suspect to eventually meet him in person. In other cases however, despite much 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 method of cooperation. Conversations and messages between suspects cover useful information about their activities, contacts, lifestyle or motives. The case files 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 thus not readable for the police with an internet tap.

In several cases the police have confiscated data carriers, which are also often protected by strong encryption. The upcoming new Computer Crime Bill offers the police new investigative tools, and creates possibilities to get access to information on these tools before it is encrypted.

Facilitators

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 preventing, detecting and involving these parties. An interesting example in this light is the ITOM project,⁹⁷ in which these new facilitators are informed and involved.

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 extremely 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.⁹⁸

Confiscation of assets

When it comes to the challenges for law enforcement in the case of Cyber-OC, the detection and confiscation of assets from suspects appear to be a difficult or time-consuming part of the investigation. In only one case was a separate financial investigation started. In other cases large amounts of money

⁹⁷ For more info see: http://www.eurojust.europa.eu/doclibrary/Eurojust-framework-ejstrategic-meetings/Eurojust%20Strategic%20Meeting%20on%20Cybercrime,%20November%202014/Report-Strategic-Seminar-Cybercrime_2014-11-20_EN.pdf.

⁹⁸ See for instance: <https://www.veiligbankieren.nl/fraude/geldezels/>.

are mentioned or seen on web accounts without knowing where they are or where they 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 investing in knowledge about money flows on the internet.

Information position 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 the High-Tech Crime Team 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.

International cooperation

The internet is a virtual place without borders. A criminal investigation on cybercrime therefore poses new challenges for law enforcement agencies. Over the last decade, substantial investments have been made in the Netherlands to intensify law enforcement on cybercrime. The investments have resulted in permanent law enforcement capacities reserved for investigating 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 also raises additional questions such as which country should prosecute the suspect, as cybercrime sometimes has no physical place.

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 the capacities 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. Owing to different priorities, complicated paper-

work or political difficulties, these requests are often dealt with at 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 cyber-criminals.

5 Concluding remarks for the Netherlands

Involvement of organised crime groups in cybercrime

Based on the Dutch cases in our sample, 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 crime, 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).⁹⁹

Secondly, there are suspects that utilise the new opportunities that the internet provides to commit traditional crimes. Within these organised crimes firstly 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 make new ways of skimming possible. 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 (ibid.).

Thirdly, the internet makes it possible to commit new online crimes. This means, for example, blocking someone's computer or performing a DDoS attack. These crimes do not exist offline. Wall calls these entirely new crimes computer-dependent crime or 'true cybercrime' (ibid.).

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 certain expertise. This can range from commissioning a hack or writing a script to more secondary roles such as de-

⁹⁹ Wall, D.S. (2005/15), The Internet as a conduit for criminals, pp.77–98, in: Pattavina, A. (ed.) *Information Technology and the Criminal Justice System*. Thousand Oaks, CA: Sage.

livering or receiving packages, channelling money to a safe destination, theft or smuggling drugs.

Using the internet to commit traditional organised crime

In our dataset 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 Dutch 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 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 see 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 criminals are able to build online relationships and collaborate

without physically meeting each other. The use of forums and other communication services allows criminals to collaborate across borders. Anonymity plays a crucial role here, as there is a relatively low risk for criminals. 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 allowed criminals to reach different targets much more easily. We can make a distinction between the types of targets, namely the victims and the customers of the criminals, in other words, people found by the criminals and those who contact the criminals. For the first type, it is important to notice the difference between what Wall (2014) calls 'technical victimisation' and actual harm.¹⁰⁰ '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 criminals with simpler new ways to reach victims. Through phishing attacks, hacked databases and different kinds of malware the criminal is able 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 criminals 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 many criminals. In addition, this may be seen as a new business idea, where the criminal 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 led 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.

¹⁰⁰ Wall, D. S. (2014), High risk cyber crime is really a mixed bag of threats. Retrieved May 2016 from: <http://theconversation.com/high-risk-cyber-crime-is-really-a-mixed-bag-of-threats-34091>.

Structural changes in organised crime

One of the general findings based on the Dutch 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;¹⁰¹ Van Koppen et al. 2010¹⁰²). 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 Dutch 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 involun-

¹⁰¹ Kleemans, E. R., Poot, C. J. de (2008), Criminal Careers in Organized Crime and Social Opportunity Structure. *European Journal of Criminology* 5 (1), pp. 69–98

¹⁰² Koppen, M. V. van, Poot, C. J. de, Kleemans, E. R., & Nieuwbeerta, P. (2010), Criminal trajectories in organized crime. *The British Journal of Criminology*, 50(1), pp. 102–123.

tarily, 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 cryptocurrencies or money transfers via web accounts that are used as a bank account to pay errand boys, 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. There are no reporting systems or controlling authorities that identify and mention unusual money transfers. This provides many opportunities for performing illegal activities.

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 (Kleemans et al, 2002¹⁰³), where knowing and involving people with certain skills or connections is crucial. These 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.

¹⁰³ Kleemans, E. R., Brienens, M. E. I., Bunt, H. G. van de, m.m.v. Kouwenberg, R. F., Paulides, G., Barendsen, J. (2002), *Georganiseerde criminaliteit in Nederland; tweede rapportage op basis van de WODC-monitor, O&B 198*. Den Haag: WODC.

There are also aspects of Cyber-OC that might differ somewhat from other forms of organised crime:

- *Anonymity in cyberspace*: online activities can be conducted anonymously, and physical 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. 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 (this is also recognised by Group IB 2011; Europol 2015¹⁰⁴). 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’.

Final remark

Knowledge about the nature of organised forms of cybercrime can help law enforcement 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

¹⁰⁴ Europol (2015), Internet Organised Crime Threat Assessment (IOCTA).

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 Cyber-OC 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.

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 complex topic of cybercrime. We would like to thank them for giving us feedback on our writing and for their patience in explaining complex digital topics.

6 References

Literature and reports

- Beijer, A., Bokhorst, R.J., Boone, M., Brants, C.H. & Lindeman, J.M.W. (2004), *De wet bijzondere opsporingsbevoegdheden: eindevaluatie* [The Act on Special Investigative Police Powers – final evaluation]. Onderzoek en Beleid 222. The Hague: Boom.
- Bernaards, F., Monsma, E. & Zinn, P. (2012), *Criminaliteitsbeeldanalyse High Tech Crime (CBA)*. KLPD: Woerden.
- 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 combatting Cyber-crime’ – Report on the Netherlands. Brussels: CotEU.
- Dienst Landelijke Recherche & Landelijk Parket (National Crime Squad & Public Prosecutors’ Office) (2014), *Tactische Programma High Tech Crime* [Tactical Programme for High-Tech Crime] 2014.
- Electronic Crimes Task Force (ECTF) Covenant, <https://www.rijksoverheid.nl/documenten/convenanten/2011/03/15/convenant-samenwerking-en-informatie-uitwisseling-electronic-crimes-task-force>.
- Europol (2015), *Internet Organised Crime Threat Assessment (IOCTA)*.
- Ferdinandusse, W.N., Laheij, D. & Hendriks, J.C. (2015), *De bewaarplicht telecomgegevens en de opsporing: Het belang van historische telecomcommunicatie gegevens voor de opsporing* [Telecoms Data Retention and Criminal Investigation: The importance of historical telecommunications data in solving crime], https://www.om.nl/publish/pages/44621/de_bewaarplicht_telecomgegevens_en_de_opsporing.pdf.

- Graaf, D. de, Sosha, A.F. & Gladyshev, P. (2013), Bredolab: Shopping in the cybercrime underworld, in: M. Rogers & K.C. Seigfriedd-Spellar (eds.), *Digital Forensics and Cybercrime*. Fourth International Conference ICDF2C 2013 (pp. 302–313).
- Inspectie Openbare Orde en Veiligheid (Inspectorate of Public Order and Security) (2012), *Follow the money!* The Hague: IOOV.
- Kaspersen, H.W.K. (1990), *Strafbaarstelling van computermisbruik* [Criminalisation of computer misuse]. Deventer: Kluwer.
- Kaspersen, H.W.K. (2004), *Bestrijding van cybercrime en de noodzaak van internationale regelingen*. JV, 08, pp. 58–75.
- Kaspersen, H.W.K. (2006), 'Jurisdiction in the Cybercrime Convention', in: Koops, E.J. & Brenner, S. (eds.), *Cybercrime and Jurisdiction: a Global Survey*. Den Haag: West Nyack.
- Kleemans, E.R., Bienen, M.E.I., Bunt, H.G. van de, m.m.v. Kouwenberg, R.F., Paulides, G. & Barendsen, J. (2002), *Georganiseerde criminaliteit in Nederland; tweede rapportage op basis van de WODC-monitor*, O&B 198. Den Haag: WODC
- Kleemans, E.R. & Poot, C.J. de (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: Corstens, G.J.M. & Groenhuijsen, M.S. (eds.), *Rede en Recht: opstellen ter gelegenheid van het afscheid van prof. mr. N. Keijzer van de Katholieke Universiteit Brabant*. Deventer: Gouda Quint 2000.
- Koops, B.J. (ed.) (2007), *Strafrecht en ICT* [Criminal law and ICT]. The Hague: SDU Uitgevers.
- Koops, B.J. (2010), *Cybercrime Legislation in the Netherlands*. *Netherlands Reports to the Eighteenth International Congress on Comparative Law*. Erp, J.H.M. van & Vliet, L.P.W. van (eds.). Antwerp: Intersentia.
- Koops, B.J. (2012), *De dynamiek van cybercrimewetgeving in Europa en Nederland* [The dynamics of cybercrime law in Europe and the Netherlands]. JV, 01: 9–24.
- Koops & Goodwin (2014), *Cyberspace, the cloud, and cross-border criminal investigation*. The Hague: WODC.
- 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.
- Koppen, M.V. van, Poot, C.J. de, Kleemans, E.R. & Nieuwebeerta, P. (2010), *Criminal trajectories in organized crime*. *The British Journal of Criminology*, 50(1): 102–123.

- Krommendijk, M., Terpstra, J. & Kempen, P. H. van (2009), De Wet BOB: Titels IVa en V in de praktijk. Besluitvorming over bijzondere opsporingsbevoegdheden in de aanpak van georganiseerde criminaliteit [The BOB: Books IVa and V in practice, decisions on special investigative powers to combat organised crime]. Uitgeverij Boom.
- Kruisbergen, E.W. & Jong, D. de, with Kouwenberg, R.F. (contrib.) (2010), Opsporen onder dekmantel [Undercover investigation], Onderzoek en beleid 282. The Hague: Boom Juridische Uitgevers.
- Kruisbergen, E.W., Bunt, H.G. van de & Kleemans, E.R. (2012), Georganiseerde criminaliteit in Nederland: Vierde rapportage op basis van de Monitor Georganiseerde Criminaliteit [Organised Crime in the Netherlands: Fourth report based upon the Organised Crime Monitor], Onderzoek en beleid 306. The Hague: WODC.
- Leukfeldt, E.R. (2014), Cybercrime and social ties. Phishing in Amsterdam. Trends in Organised Crime, 17: 231–249.
- Leukfeldt (2015), Organised Cybercrime and Social Opportunity Structures: a Proposal for Future Research Directions. The European Review of Organised Crime, 2(2).
- Ministerie van Veiligheid en Justitie [Ministry of Security and Justice]. Veiligheidsagenda [Security Agenda] 2015–2018. The Hague: Min. VenJ.
- NCTV – National Coordinator for Security and Counterterrorism (2013), NCSS – National Cyber Security Strategy 2. The Hague: NCTV. URL: https://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 capital for business: an evaluation of the criminal confiscation legislation – final report]. The Hague: WODC.
- 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 Use of Telephone and Internet Taps in Criminal Investigation], Onderzoek en Beleid 304. The Hague: Boom Lemma.
- Odinot, G., Jong, D. de, Bokhorst, R.J. & Poot, C. de (2013), The Dutch Implementation of the Data Retention Directive. The Hague: WODC/ Boom Lemma, https://www.wodc.nl/images/ob310-summary_tcm44-534135.pdf.
- OM (Openbaar Ministerie) (2015), OM Meerjarenplan Cybercrime [Public Prosecution Service Long-Term Plan for Cybercrime] 2015–2018.
- Stol, W.Ph., Leukfeldt, E.R. & Klap, H. (2012), Cybercrime en politie. Een schets van de Nederlandse situatie anno 2012. JV, 01.

- Struiksmā, N., Vey Mestdagħ, C.N.J. de & Winter, H.B. (2012), De organisatie van de opsporing van cybercrime door de Nederlandse politie. Amsterdam: Reed Business. URL: <http://www.politieenwetenschap.nl/cache/files/55f6cc2b539f1Cybercrime.pdf>.
- Tak, P.J.P. (2008), The Dutch Criminal Justice System, third edition. Nijmegen: Wolf Legal Publishers.
- Van der Hulst, R. & Neve, R. (2008), High-tech crime, soorten criminaliteit en hun daders. Een literatuurinventarisatie [High-tech crime, different crime types and perpetrators: A literature review], Onderzoek en beleid series. The Hague: WODC/Boom Lemma.
- Van der Leij, J.B.J. (2014), Het Nederlandse strafrechtssysteem [The Dutch criminal justice system], in: Criminaliteit en Rechtshandhaving 2013, Ontwikkelingen en samenhangen [Crime and law enforcement 2013, developments and cohesion]. WODC, Boom Lemma.
- Wall, D.S. (2014), High risk cyber crime is really a mixed bag of threats. Retrieved May 2016 from: <http://theconversation.com/high-risk-cyber-crime-is-really-a-mixed-bag-of-threats-34091>.
- Wall, D.S. (2005/15), The Internet as a conduit for criminals, pp. 77–98, in: Pattavina, A. (ed.) Information Technology and the Criminal Justice System. Thousand Oaks, CA: Sage.
- Wervingsfolder Politie [Police recruitment brochure] 2013.
- Wiemans, F.P.E. (2004). Onderzoek van gegevens in geautomatiseerde werken [Investigating data in computerised devices and systems], (diss. Tilburg). Nijmegen: Wolf Legal Publishers.

Case law

- Hoge Raad (Supreme Court of the Netherlands), 11 October 2005, LJN AT 4351.
- Rechtbank Rotterdam (Rotterdam District Court), 26 March 2010, LJN BM2520
- Hof 's-Gravenhage [The Hague High Court], 27 April 2011, LJN BR6836.
- Rechtbank Den Haag (The Hague District Court), 11 March 2015, ECLI:NL:RBDHA:2015:2498

Parliamentary papers

- Kamerstukken II [Dutch parliamentary document] 2004/05, 26 671, no. 10.
- 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>
- Kamerstukken II [Dutch parliamentary papers] 2013–2014, 33 930 VI, no. 1.

Web links

- Convention on Cybercrime, par. 193. <http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures>.

<http://www.dutchcowboys.nl/cybercrime/politie-en-cybercriminelen-zijn-op-zoek-naar-medewerkers-met-dezelfde-vaardigheden>; accessed July 2015.

<http://computerworld.nl/beveiliging/79823-torrat-bende-anoniem-door-gebruik-vpn-en-bitcoins>.

<http://www.bbc.com/news/technology-18189987>.

http://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/>.

http://www.eurojust.europa.eu/doclibrary/Eurojust-framework/ejstrategic-meetings/Eurojust%20Strategic%20Meeting%20on%20Cybercrime,%20November%202014/Report-Strategic-Seminar-Cybercrime_2014-11-20_EN.pdf.

III. Cyber-OC in Sweden

Y. Werner, L. Korsell

ICT-related crime is often perceived as a new crime phenomenon (Brå 2000). But is it really that new? In 1981, Brå published one of the first scientific works in Sweden on the area and already then it was discussed whether or not computer crime should be considered a traditional crime or a new phenomenon (Brå 2000, Brå 1981). Then, before the internet era, ICT-related crime mostly concerned embezzlements carried out through insiders. The mainframe was in its prime and all focus was on its security (Brå 2000). It was not only criminologists, lawyers and computer specialists who had become aware of the rising problem (Brå 1981). The authors of the report also established that the vulnerability of computer systems had come to the attention of the Swedish government through several governmental commissions, the first one already during the late 70s (ibid.).

During the next decade, the heavy and stationary mainframe, only used by large businesses and the public sector, was replaced by the personal computer and ICT became more accessible to the commonage. Networks were growing and 'the hacker' was in the media's focus (Brå 2000). In 1985 the Swedish police formed its first ICT-crime group with the specific responsibility of investigating ICT and computer-related crimes (Goldberg, Larsson 2011: 291–293). In the early 90s, the same year as the first Swedish hacker group, 'the Swedish hacker association', were arrested (Goldberg, Larsson 2011: 291–293), another governmental commission (SOU 1992) was carried out on the subject. The findings showed that computer crimes were not widely committed; however, they found unauthorised copying of software, hacking and viruses to be largely present (Brå 2000).

The latter half of the decade brought an increase in attention towards Swedish hacker activity. In 1996 a Swedish hacker group called 'Power Through Resistance' hacked the website of the American Central Intelligence Agency (CIA) as a protest against the ongoing trial against 'the Swedish hacker association'. Shortly thereafter, the Swedish police together with the FBI arrested a third hacker group ('Fragglarna') based in Sweden, after multiple hacking attacks against the US Air Force and NASA.

As said, ICT became more accessible to the public during the 80s and the usage of computers and the internet has continued to increase during recent years (SCB 2014). Today, 99% of Swedish households and companies can gain access to mobile broadband (SOU 2015) and three quarters of the population aged 16–85 use computers and the internet on a daily basis. The most common areas of usage are information searches, email, internet banking and e-shopping (SCB 2014, PTS 2013). As highlighted by a governmental commission in 2015, to prevent cyber incidents and cybercrime, society's awareness and understanding regarding cybersecurity needs to be raised (SOU 2015).

1 Context information

1.1 The character of cybercrime in Sweden

What no one during the early years of cybercrime studies could foresee was the rapid growth of the internet. The development within information and communication technology has created new possibilities for everyone, criminals included (SOU 2015). This has, of course, had an effect on what cybercrime is perceived to be today. If the focus in the early days was on embezzlements, mainframes and hackers, the spectrum has now been broadened.

One can argue that most crimes today have a cyber connection (ibid.). This is obviously the case for crimes that by their nature require modern technology, such as computer fraud and hacking. But modern society and its dependence on high-tech communication is such that even crimes such as claimant fraud, credit card fraud and false invoices have ICT elements almost by definition. The last study made by Brå concerning cybercrime in general in Sweden was made in 2000. Then, most ICT-related crimes had an ‘everyday nature’, i. e. it was a question of traditional crime in an ICT environment (Brå 2000). There were no clear signs of organised crime embracing the latest technology such as hacking, but the internet and other ICT structures were identified as being increasingly used as channels of communication (ibid.). Later, a study made in 2009 showed that cyber criminals often tend to organise themselves in business-like networks with clear international connections, where external experts – people with the right knowledge and ability – are recruited temporarily to perform specific functions (Brå 2008), a trend that is still prevalent (FRA 2015, Kronqvist 2013: 213). Another result from the same study that likewise has not changed is that one of the most common motivations of the offenders within cybercrime is financial gains (Brå 2008, MSB 2015). In 2015, when a governmental commission regarding cybersecurity problematised the risks following dependence on ICT, cybercrime was described as being committed by people without criminal premeditation, by hacker groups, activists and criminal organisations and by states. The report also described the offenders as either resourceful with a high level of competence or the opposite – they may just have downloaded the information and tools needed to commit the act.

1.2 Development over time

Even if the latest study found cybercrimes to have an ‘everyday nature’ (Brå 2000), the number of advanced cyberattacks directed against important institutions in Sweden, such as corporations, universities and government agencies, has increased in number and complexity over the past few years. These

attacks are mostly performed by resourceful actors, such as other countries' intelligence services or large criminal networks, and the intention is usually to obtain sensitive information through the usage of malicious code (FRA 2013, Säkerhetspolisen 2012). It is not only the scope of these attacks that has changed, but also the attackers' behaviour. Compared to the protest hacking attacks, performed to draw attention to a specific cause, today's use of hidden malicious codes is constructed so as not to be detected at all (FRA 2011).

Even if the results found in 1981 differ from contemporary cybercrime, both in character and prevalence, many of the summarising thoughts are still relevant today (Brå 2000). For example, the report highlighted the complexity that ICT brings regarding anonymity and it concluded that the majority of the people who committed computer crimes were not the typical criminal. Instead, the computer crime was usually the first recorded criminal activity of the person. Lastly, but maybe most interestingly in relation to this study, they found that 50% of the computer-related crimes were carried out in collusion (Brå 1981).

1.3 Swedish penal legislation

Swedish penal legislation is in many ways neutral to technique and there are few sections of the law concerning ICT. These sections will be covered in this chapter and they concern both 'pure' ICT crimes and legislations and rules in relation to ICT connections and organised crime.

Firstly, there is 'computer fraud' in the Criminal Code chapter 9, section 1, second paragraph. There are two main criteria for committing fraud according to the regular section. The first one is that the deed has to concern the misleading of a natural person. When it comes to computers or other kinds of 'automatic processes', it is not the natural person who has been misled but the machine. Secondly, the misleading element must therefore be that the perpetrator gives wrong or incomplete information, or changes a program or recording, or in another way unlawfully influences an 'automatic data processing or similar automatic process'.

The second typical computer crime is 'hacking' or, more correctly, 'computer intrusion' in the Criminal Code chapter 4, section 9c. The criteria for computer intrusion are getting unlawful access to information in connection with automatic data processing, or modifying, deleting or blocking information, or enrolling information in a register.

In relation to ICT, a crime very much connected to computers and the internet is ‘contacting a child for a sexual purpose’, often referred to as ‘grooming’, in the Criminal Code chapter 6, section 10a.

In relation to the investigative work of ICT-related cases, the Data Retention Directive was established in 2012 and obliges telephone network operators to store traffic information for six months.

Beyond this, references to organised crime in Swedish penal legislation are scarce. However, the Criminal Code chapter 29, section 2, which is a general rule for aggravating factors, highlights acts that are committed in an organised or systematic way as well as those that are rigorously planned (in paragraph 6). Thus, organised crime is viewed as an aggravating factor.

1.4 Statistics

The general picture is clear, cybercrimes are increasing rapidly and there is nothing to indicate that the trend is slowing down (RPS 2014). At the same time, there is no data on the extent of reported crimes that are committed via the internet (Brå 2015a).

The crime statistics are produced based on codes that are used by the police when registering reports (SCB 2011). Of these codes, only seven concern cybercrime: hacking, computer fraud, internet-assisted fraud, (computer) sabotage, internet-related child pornography crime, copyright infringement through file sharing and crimes against industrial property rights with the help of the internet (Brå 2012b). However, practically no codes show whether the crime occurred over the internet (Brå 2015a). This leads, for example, to a receiving offence committed through a website being registered as ‘only’ a receiving offence (RPS 2014). In this way, most of the crimes that are cyber-related are not registered as such.

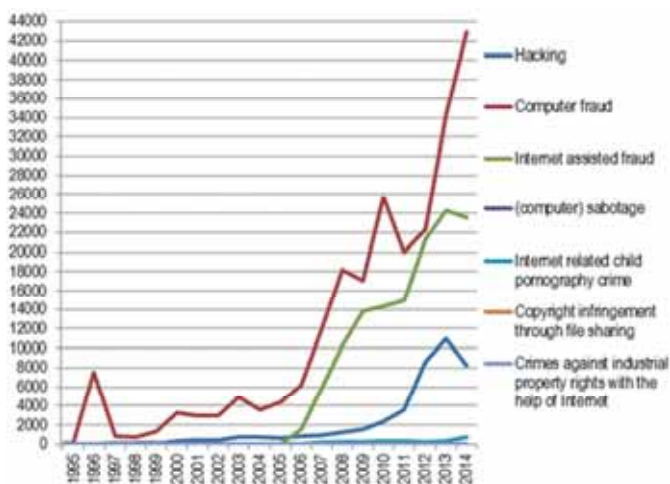
Table 2: Reported crimes

Year	Hacking	Computer fraud	Internet assisted fraud	(Computer) sabotage	Internet related child pornography crime	Copyright infringement through file sharing	Crimes against industrial property rights with the help of Internet
1999	9	1 325	-	70	-	-	-
2000	341	3 304	-	65	-	-	-
2001	407	2 970	-	52	-	-	-
2002	393	2 927	-	63	-	-	-

Year	Hacking	Computer fraud	Internet assisted fraud	(Computer) sabotage	Internet related child pornography crime	Copyright infringement through file sharing	Crimes against industrial property rights with the help of Internet
2003	731	4 939	-	69	-	-	-
2004	720	3 588	-	61	-	-	-
2005	627	4 361	-	39	-	-	-
2006	849	6 236	1 502	49	54	-	-
2007	908	11 956	5 860	55	272	-	-
2008	1 282	18 173	10 260	44	272	-	-
2009	1 493	17 092	13 800	37	252	-	-
2010	2 346	25 668	14 350	39	299	19	13
2011	3 597	19 960	14 927	41	319	41	14
2012	8 646	22 359	21 354	44	268	40	10
2013	11 010	34 284	24 224	25	361	37	6
2014	8 200	42 883	23 528	20	738	27	9

Source: Statistiska Centralbyrån (SCB), URL: http://www.scb.se/sv/_Hitta-statistik/

Figure 5: Reported crimes



Source: Statistiska Centralbyrån (SCB), URL: http://www.scb.se/sv/_Hitta-statistik/

Even if there are no official statistics on cybercrime or cyber-related crimes in general, the clear-up rate of those crimes is generally low (RPS 2014) and they are estimated to cost hundreds of millions of dollars a year (838 million in 2013) (MSB 2015). A possible partial explanation of the low clear-up rate is that frauds generally have a very low rate of clearance and that frauds constitute a significant proportion of cyber-related crimes (Brå 2015b).

1.5 Political agenda

Table 3: Law enforcement and related authorities in Sweden

Authority	Abbreviation	Explanation
The National Radio Establishment	FRA	The Swedish national authority for Signals Intelligence
The Swedish Police Authority	The Police	
The Swedish Security Service	Säpo	Security agency with the focus on national security
The Swedish Armed Forces		Responsible to prevent and manage conflicts and wars
The Swedish Civil Contingencies Agency	MSB	Responsible for issues concerning civil protection, public safety, emergency management and civil defence
The Swedish Customs		Responsible for managing trade and law enforcement
The Swedish Post and Telecom Authority	PTS	Monitors the electronic communications and postal sectors in Sweden

Source: Compiled by the author

To understand the context in which Cyber-OC operates, the political agenda of cybersecurity will be presented below. This concerns cybersecurity on a general level and not specifically in relation to organised crime. The general approach to ICT might be a shortcoming since it lacks a focus on specific crime areas and offenders.

In 2015 the governmental commission ‘Cybersecurity in Sweden – strategy and measures for secure information in central government’ was presented. The study had been commissioned by the government to recommend a national strategy for the management and transmission of information in electronic communication networks and IT systems. The proposal was also commissioned to include overall goals for the information security of the public and recommendations on how Sweden is to maintain its security and integrity

in important public IT infrastructures (SOU 2015). The result of the commission can be summarised in six overall goals that Sweden has to work towards: (1) to strengthen regulation and supervision, (2) that the state should establish clear requirements for procurement in the ICT area, (3) that governmental authorities should communicate securely, (4) that all governmental agencies should report cyber incidents, (5) to strengthen efforts to prevent and combat cybercrime and (6) that Sweden should be a strong international partner in questions regarding this area. The report also suggested that the government should strengthen and coordinate its efforts to promote Sweden's position in international collaboration on ICT and cybersecurity (ibid.).

To achieve these goals the commission suggested specific actions. In order to strengthen Swedish efforts in combating and preventing cyber incidents and cybercrime, the following three areas should be managed in particular. First of all, the commission emphasised that Sweden should conclude the ratification of the Council of Europe Convention on Cybercrime, which Sweden signed in 2001. The government also needs to consider whether a regulation can be introduced to the Public Access to Information and Secrecy Act whereby secrecy can be maintained regarding information that is exchanged between law enforcement agencies and other agencies involved in law enforcement work within the area of cybersecurity. A review of the provisions on coercive measures in Chapters 27 and 28 of the Swedish Code of Judicial Procedure and other sections of law shall be conducted to ensure that law enforcement agencies are able to carry out their activities in the digital environment.

The commission also emphasised that measures towards increased collaboration, customised legal support and well-developed expertise are needed in order to create opportunities for law enforcement authorities to successfully detect, prosecute and investigate crime in the digital environment. Furthermore, to prevent cyber incidents and cybercrime, the commission states that the state has to raise awareness and understanding throughout society by spreading information on information security. This can be done through education, research and development (ibid.).

1.6 The police organisation

There are seven geographical police regions in Sweden, all responsible for the overall policing in their area. In general, decision-making should be conducted at the lowest appropriate level in the hierarchy, but there are some specific essential areas that are kept together at a regional level e.g. the investigation of certain types of crime, among them cybercrime (ibid.). Thus, every region has its own IT forensic capacities within the investigation unit where

cyber-related crimes are handled as well as its own unit for internet intelligence, where internally trained employees work with active surveillance on the internet in various fields, e.g. drug sales. (Polismyndigheten 2014:12).

As said, there are also two separate national departments: The first of these is the National Operative Department, whose work does not involve any self-initiated operational activities. They should instead work in support of the police regions. They also have a national responsibility to control, develop and monitor operations and ensure their consistency in specific areas, e.g. complex cybercrimes. The second separate department is the National Forensic Centre. They should, amongst other things, perform forensic investigations and one of the four expertise units is solely designated to handle information technology (Polismyndigheten 2015a).

1.7 Measures by the police

Through well-established contacts with the Swedish Federation of Trade, different banks and authorities as well as through information spreading on Facebook, the police are working to combat cybercrime (RPS 2014). This was emphasised as a positive example of crime prevention in a supervision report commissioned by the police. The report, with the purpose of evaluating the ability of the police to handle ICT-related crimes, also found a lack of coherence within the working procedures. For example, they worked with a narrow view of what cyber-related crimes were and the ICT relevance in all types of crimes was not seen. They also lacked national guidelines for methodological support and crime prevention regarding these sorts of crimes (ibid.). Other areas that were in need of improvement were the standard of ICT forensics. The report suggested adopting a common standard for training, equipment and methodology in this area. It was also recommended to consider establishing a national cybercrime centre (ibid.).

The National Operative Department with its specific role in relation to complex cybercrime has been established. A new national cybercrime centre, with the purpose of providing expert resources in this area, is being set up and will be running from October 2015 (MSB 2015).¹⁰⁵ Furthermore, during 2015 the National Operative Department is conducting a preliminary study regarding crime prevention in relation to ICT-related crimes, which will form the basis for future initiatives.¹⁰⁶

¹⁰⁵ <https://polisen.se/Aktuellt/Nyheter/2015/Jan/Sa-ska-polisen-bekampa-it-brotten/>.

¹⁰⁶ Förstudiedirektiv, Polisen, Diariennr: A105.564/2015.

2 Methodology

2.1 Selection of cases

Owing to the lack of official criminal codes concerning internet as a crime scene and ICT as means of crime, there is no databank of cyber-related crimes besides the seven mentioned above. There are thus no comprehensive official statistics and therefore there is no databank on the extent of organised crime, regardless of the involvement of ICT or not (Brå 2012c).

The Swedish research project was therefore obliged to rely on a snowball process in the first step of collecting cases. Four areas of focus were central in selecting relevant cases. First of all, the aim was to get as wide a spread of crime types as possible as well as a geographical dispersion. The selection of cases was also based on the amount of information accessed in the police prosecution files. This means that cases from which one could get as much information as possible regarding the persons, *modus operandi*, profit, etc., were prioritised. Lastly, the latest cases possible were selected.

The first step in finding data was to contact ‘key persons’, i. e. persons within law enforcement authorities whom we had identified as working actively within the area of cyber-related crime. We described our criteria and definitions and asked for cases that they could think of. During the process of coding, we also continued to search for cases in order to fill information gaps that were found. This was done through contact with key persons but we also subscribed to newsletters from various law enforcement authorities to obtain information on new cases.

The last step was to gather a reference group consisting of people who work in the field of cyber-related crime but who had not been involved in our first step of collecting cases. The reference group was organised as a seminar to promote discussion. The purpose of this reference group was for them to work as a control group and to see if our picture was consistent with their view of reality. If not, they could comment on which areas or circumstances had been missed and maybe even propose further cases representative for those areas. The seminar was very fruitful and gave information to bear in mind as well as a new case to code. In total, fifteen cases are included in the study.

2.2 Information available in police or prosecution files

Regarding the hard information, it is all well documented and included in the files: Information on gender, age, nationality, address, work situation, economic status and education as far as possible; interrogations with suspects;

protocols of house searches and confiscations; analysis of programs and technical devices; official mail.

2.3 Expert interviews

Seven expert interviews were conducted with people working within different law enforcement agencies and with varied tasks. The interviewees are employed by the police, the prosecution service and the Swedish customs, and their work involves investigation, prosecution, forensics and development in relation to cyber-related crimes.

2.4 The cases

The cases included in the study are presented in the chart below with information concerning crime description, cyber category, number of suspects, OC criteria fulfilled and categorisation: whether it is a case of traditional organised crime that enters the internet ('enters') or organised crime that develops in an internet environment ('develops').

Table 4: Analysed cases

No.	Crime description	Cyber category	No. of suspects	OC criteria	Categorisation	Reference
1	copyright infringement through file sharing	computer-assisted	4	1, 2, 3, 5, 6, 8, 11	develops	K1
2	fraud through Trojans	computer-assisted computer content	24	1, 2, 3, 5, 6, 11	develops	K2
3	fraud through hacking databases	computer-assisted computer content	10	1, 2, 3, 5, 6, 11	develops	K3
4	fraud through wireless remote console	computer-assisted computer content	8	1, 2, 3, 5, 6, 11	develops	K4
5	fraud through credit card information	computer-assisted	4	1, 2, 3, 5, 9, 11	develops	K7
6	credit card fraud through forgery of documents	computer-assisted cryptomarkets	10	1, 2, 3, 4, 5, 6, 7, 11	develops	K8
7	drug offence and financial crime	computer-assisted	9	1, 2, 3, 5, 6, 8, 9, 11	enters	K9
8	various drug-related offences	computer-assisted	21	1, 2, 3, 5, 6, 8, 9, 11	enters	K10

No.	Crime description	Cyber category	No. of suspects	OC criteria	Categorisation	Reference
9	conspiracy to traffic and pimp	computer-assisted	9	1, 2, 3, 4, 5, 6, 7, 9, 11	enters	K12
10	extortion and fraud	computer-assisted	4	1, 2, 3, 5, 7, 11	enters	K13
11	copyright infringement	computer-assisted	3	1, 2, 3, 5, 6, 8, 11	develops	K14
12	illicit gambling and financial crime	computer-assisted	14	1, 2, 3, 4, 5, 6, 7, 8, 11	enters	K16
13	illicit gambling	computer-assisted	15	1, 2, 3, 5, 6, 8, 11	enters	K17
14	fraud through credit card information	computer-assisted cryptomarkets	20	1, 2, 3, 5, 6, 9, 11	develops	K18
15	various drug-related offences	cryptomarkets	3	1, 2, 3, 5, 6, 8, 11	develops	K19

Source: Presentation by the author

3 General description of the Swedish sample

Owing to the multiple variations in the crime types and modus operandi in the selected cases, the general description will have its emphasis on the general aspects. There are some reoccurring structures and traits of character that will be described but we will also focus on what we did not see.

3.1 Visible characteristics

The first impression of the majority of the cases is that they consist of rather small-scale criminal procedures. By small-scale, we mean a number of things and these will be explained below.

3.1.1 Persons

Small-scale is firstly a question of the number of persons involved. There were cases of up to 24 suspects and cases with three suspects. There are five cases of groups involving more than ten suspects while ten cases involved ten or fewer suspects. When cases involve numerous people, it is usually two or three people that are involved in the entire criminal procedure. The rest are

periphery members. The core of two to three members does not seem to decrease in number when the total number of suspects is lower.

3.1.2 Structure

The majority of the cases had a hierarchic structure of some sort. This was either a question of a two-level hierarchy, where a person is either a part of the decision-making group or not, or it involved a structure of four or five different levels. The hierarchies were sometimes examples of classic pyramids and sometimes more spherical in their organisation. We also saw examples of different individual and smaller hierarchic groups collaborating.

3.1.3 Modus operandi

The second aspect that we refer to when talking about small-scale procedures is the complexity of the set-up. There are almost no cases with a recruitment of strategically key persons that has a significant bearing on the set-up. There are only a few cases where the people involved had to move or change their day-to-day life in order to carry out the criminal activity. We found cases where the suspects had operated within and started legal businesses for criminal functions. However, starting a company is a very easy process and something anyone can do. Lastly, the set-ups consisted of basic, simple and few steps. Thus, the criminal activity was quite isolated and the groups were, in the majority of the cases, in control of the majority of the process themselves.

3.1.4 ICT

The third aspect in relation to the small scale is the level of ICT knowledge needed by the criminal groups. The majority of our cases were cyber-assisted crimes. They were not technically advanced and only four cases needed special ICT competence. In those cases in which such knowledge was required, the group was mostly able to buy that knowledge in the form of a service from someone online or under the cover of a legal business. Thus, most of the cases in this study involve procedures and measures that anyone, regardless of technical skills, could have carried out.

3.1.5 Motive

In terms of the motive or aim of the criminal activity, we did not see a single case that did not involve economic gain as an impetus. It was mostly a ques-

tion of solely economic intentions but in those cases in which other motives were present, e.g. when the suspects viewed the activity in terms of ideology or as a technical challenge, there was an economic intention as well, even if it was a question of a secondary motive.

3.1.6 Damage

When calling it small-scale, we are not referring to the damage of the crime. Despite the small numbers of people involved, the basic set-ups and the low level of ICT skills needed, the damage of the crimes is usually global and includes, for example, large sums of money lost and personal distrust towards systems.

To summarise the fifteen cases studied, they usually (1) involve a small number of members, (2) are hierarchically structured, (3) consist of rather basic set-ups with just a few steps, (4) are based on basic technical skills, (5) are profit-driven and (6) result in global and vast damage in terms of material and immaterial harm.

3.2 Invisible characteristics

We also stated that we would focus on the features that we did not see. So with the last section in mind, where are the grand hacker attacks fit for a Hollywood production? In all seriousness, does Sweden not have large-scale, technically advanced Cyber-OC? Or is it a question of the project's criteria and selection process?

Two aspects, related to the above-mentioned questions, emerged through the data collection and need to be highlighted.

First of all, the definition used for the term organised crime includes the fact that at least three people are involved in the criminal activity. This means that set-ups involving multiple persons, but where only one or two have been brought to trial and convicted, were not included in our material. In the area of Cyber-OC, especially since Crime-as-a-Service is a growing phenomenon, this raises a fundamental question as to how to count the persons involved. For example, one person hacks the police database of persons with protected identities. To be able to do this, he has bought one type of software from a second person and another type of software from a third person on the dark web. The hacker then sells some of the information to two persons who use the data to hijack identities. The 'hijackers' are then caught, arrested and prosecuted – but how many persons are actually involved? Should one count the hacker they bought the information from? And should the trial include the

two individual sellers of the software as well? When people are independently involved, how many steps in the chain should be included?

The second aspect regards the global character of Cyber-OC. As an example, Google becomes the victim of a denial of service attack. The investigation shows that there is one Swedish citizen, together with hundreds of Americans, British, Spanish and French citizens that have carried out the attack. The Swedish citizen will be prosecuted in Sweden and charged for his or her individual involvement in the attack. This is a case of Cyber-OC but owing to the fact that boundaries of legislation are national while criminal activity is global, a comprehensive approach is lacking. In relation to our study, that case would not have been part of the data collection since it is only addressing one individual's own actions.

3.3 Typology

There are various ways of classifying the different aspects of Cyber-OC. Besides the typology used in our project, three other areas of focus in relation to ICT became evident through our research and analysis.

3.3.1 Group

The first classification is based on the rootedness and geographical structure of the criminal group, as well as how they use ICT in relation to this. Below three categories will be presented: the locals, the glocals and the spatial networks.

The locals

The locals are groups based in a specific relatively small geographical area. This means that every person involved in the group is personally active, living and working in this specific town or city. Hence, recruiting is a local matter, where only friends, acquaintances or other people from the same place can get involved. The locals do however use ICT to reach outside their geographical area to commit crime, and the only relation the group has to 'the outside world' is thus in terms of victims.

An example of this might be a criminal group who obtains credit card information online to commit fraudulent purchases or fraudulent transfers from the victims' accounts. The group is personally active from a small area but with the help of the internet, they can commit crimes that affect people all over the world.

The glocals

The name 'the glocals' reflects the term 'glocalisation' and its aim to combine the idea of globalisation with that of local considerations. These groups are mainly, and at a first stage, locally based but unlike the locals, they use the forces of globalisation in relation to recruitment and activity. This means that the base and main idea of the criminal group emanates from a local point. However, to be able to commit the crime, they need to use ICT in several steps of their *modus operandi*. This is mostly a question of recruitment and global contacts, as well as relating to communication from time to time. Thus, the glocals only control limited parts of the criminal procedure, while other parts are outsourced or bought through the internet.

An example of this is a criminal group selling illegal medication online according to the following procedure. Three persons living in a town in Sweden decide to start an online pharmacy selling medicine that is classified as narcotics by Swedish law. Firstly, they need to construct a website. This is done through the online recruitment of a person with this knowledge. They then want to place this website on a server. Since what they are doing is illegal in Sweden, they will contact a foreign company with servers located abroad. They then need to find a supplier and a chain of production and will thus recruit a person living in a country where the prescription is legal or send someone to live there. That person will then purchase packages and send the orders at the group's request. The core group is thus locally based, while their website constructor, server, executor and activity are globally scattered. They are also utilising the differences between national legislations and the possibility of globalisation to make a profit out of it.

The spatial networks

This name also refers to an already coined term. In short, and in line with what we focused on, spatial networks consist of nodes and hubs, which according to Manuel Castells, are not spaceless but their logic is (Castells 1999: 412–413). In our typology, this means that the people and ICT equipment necessary for a crime can be, and are, located all around the world without the geographical position affecting the criminal activity. The structure of the group is thus in itself dependent on ICT.

This includes the example of a file-sharing community, where people all around the world digitalise information to enable the uploading and downloading of, for example, films and to facilitate the administration of such a site. Here, the persons as well as their computers are equal parts of a network where the information, i. e. the material being shared, is not affected or influenced by the geographical positions of the actors at all.

3.3.2 Crime type

This categorisation, used throughout this report, is based on the background of the crime type carried out by the criminal group and how that affects the role of ICT.

Traditional organised crime that enters the internet

The type of criminal activity that can be categorised as traditional organised crime that enters the internet involves crime types usually referred to as traditional organised crime. This includes trafficking, drug smuggling and extortion, the sale of counterfeit goods and illicit gambling, i.e. crimes with economic gains. The ICT element of the crime has contributed to the effectiveness of the offence but not changed its characteristics comprehensively. ICT is thus used as a tool in order to gain advantages and is replacing former procedures, usually with the consequence of making the crime more global.

Organised crime that develops in an internet environment

As the title of this category suggests, these crime types are dependent on ICT. They can be completely new crimes invented simultaneously with technical development and not having a predecessor, e.g. computer hacking. But they can also be offences that have a traditional mode but when using ICT the performance and scope of the crime changes comprehensively. For example, file sharing and violation of copyright law, which could be seen to have a traditional prototype in the sale of counterfeit goods. By digitising the access, the information is given a global reach and the economic loss of the plaintiff company is dramatically larger. Thus, in these cases, ICT is an integrated part of the entire *modus operandi*, where most of the criminal activity is committed through or reliant on computer or internet-based methods.

3.3.3 The cyber lift

Closely related to the above-mentioned categorisations is a spin-off of what David Wall calls the cyber lift. This categorisation relates to the impact of ICT and its contribution to the reach and profit of the offence. It is all based on the question of ‘what happens if the cyber aspect is excluded?’

Local level

In this first category, the answer to the question asked above is ‘the crime will be viable on a local level’. For example, fraud has been committed in various forms throughout history. Today, it is mostly a question of hacking databases, skimming, phishing or Trojans, i.e. with a method dependent on ICT. So

what happens if it is taken away? A traditional and non-ICT-related version of credit card fraud or fraudulent purchases could be cheque fraud – a purchase made with someone else's money through an illegal usage of the victim's information. Another example, which happened not too long ago, was a film company being hacked for unknown reasons. The hacker(s) gained access to a film that had not been released and published it. Could this have been committed without the use of ICT? Well, let us say that a person in the 1940s did not want a film company to get revenues from an upcoming film since the person in question thought he was entitled to the money. He could, theoretically, break into the company, steal the tapes, and show it at his own cinema. Hence, as soon as ICT disappears, these versions become more reliant on local efforts and actions. In addition, the profits of the crime are also reduced to a local level.

Non-existent

This category would instead answer the question with 'it would not be possible to commit the crime'. An example of this is a denial of service attack. These types of attacks are usually carried out in protest against a company for something that they have sided with, either in practice or in speech. The attackers thus, in different ways, overload the company's website to the point of collapse. Depending on the company's purpose, a shutdown of their site could result in lost revenue, bad publicity, security issues, irritation and costs for repairing it. So would this be able to happen without ICT? Well, let us say that a newspaper in the 1910s printed an article concerning women's right to vote. For some reason, this upset the readers and they started expressing their opinion towards the newspaper in a similar way to the attackers in a denial of service attack: by visiting the newspaper's office at the same time repeatedly. Would this protest cause the newspaper company to involuntarily shut down? Probably not.

4 Empirical findings

Owing to the wide range of Cyber-OC and its crime types, there are several variables and phenomena that are different from case to case. In order to present the results in a coherent and informative way, the findings are structured based on the division made in the analysis system:

- Traditional organised crime that enters the internet
- Organised crime that develops in an internet environment

This will be the overall division of the next sections, followed by the division of smaller characteristics based on different variables within the topic.

4.1 Characteristics of suspects and groups in Cyber-OC

In this section, the 15 Cyber-OC groups will be described in terms of the personal background of the suspects, the recruitment process, the initiation of the group and the crime, the preliminary and secondary crime type, the structure and motivation of the groups, as well as their usage of companies.

4.1.1 Traditional organised crime that enters the internet

Background

It is not easy to define the typical persons behind the kind of criminal activity that can be described as traditional organised crime that enters the internet. However, we can elaborate on this based on three variables concerning age, occupation and previous convictions.

First of all, one can see that the members included in our study are quite homogeneous in age within the groups, i.e. there are younger groups and there are older groups. For example, one group had an average age of not even 18 while another group averaged 43.5 years.

Furthermore, out of the six cases that belong to the category described as traditional organised crime that enters the internet, more than half of the suspects are employed or have their own company and barely anyone works within ICT areas. The few who do are, for example, consultants in online marketing or IT technicians and have rather mainstream knowledge and cannot be regarded as ICT experts.

Moreover, even if the average studied suspect included in this category does not have a criminal record, there are quite clear clusters within the groups who have been convicted before. Just as the ages within the groups are homogeneous, so is the criminal history of the suspects. The majority of those with a criminal record had been sentenced for minor offences such as traffic violations, shoplifting and minor drug possession. These were usually involved in the periphery of the criminal group, for example as mules. The core of these six groups by contrast had, if convicted, been sentenced for more serious crimes, usually an offence corresponding with the crime they are accused of in this current case, e.g. human trafficking, procuring or smuggling narcotics and the sale of narcotics.

Recruitment

Furthermore, the collected data shows that these people are usually recruited by family members, close friends or acquaintances. One can see that when a group is expanding, they will first and foremost look to their environment for

new members. The further away a group member is from the inner circle or the clique with the most power or knowledge of the activity, the looser the friendship or family bond also is in relation to the people in charge. If one looks at the larger groups present in this study, one can see that the centre of the group usually consists of family members, close friends or childhood friends. The next step, the ones who are close to the centre but who do not constitute the leaders can be younger family members, friends of friends or friends of the members on this level. Lastly, the most periphery members do not have any strong bonds with the leaders of any kind. Instead, these six cases show that they are usually recruited because of personal information that the other members have obtained. It may be that one person in the group knows that they have economic issues or they may be involved as a favour.

Of course, the smaller groups in this study, sometimes consisting of only three or four members, do not necessarily have this clear subdivision owing to the small number of members. However, the same applies here: the closer the person is to the people in power, the closer the friendship or family relationship. Overall, there are limited traces of recruitments online. Information regarding the occurrence of online recruitment was mostly obtained through the expert interviews and very few and brief examples were seen in the cases. However, in these very few instances the recruitment process was usually carried out through online forums where the group had advertised for an experienced individual for a specific task.

Initiation

The last section regarding the background of these groups concerns the initiation of the cyber-related criminal activity. Three scenarios are evident in the data. In the majority of these six cases, the group existed prior to the cyber-crime. The most common occurrence is that the group had been involved in a crime type of traditional character, e.g. drug smuggling, and then started selling the drugs online instead of on the streets. Secondly, there are examples of a sequence of events, where the idea of a crime arose prior to the existence of the group. However, that is not nearly as common as its opposite. The last scenario involves multi-criminals: groups who are involved in several different types of crimes. In our study, this is represented by case K12: a group that was first involved in trafficking and later entered ICT platforms and committed the offences through internet-based tools. At the same time as their trafficking activity entered the internet, they also started to install skimming machines on cash dispensers.

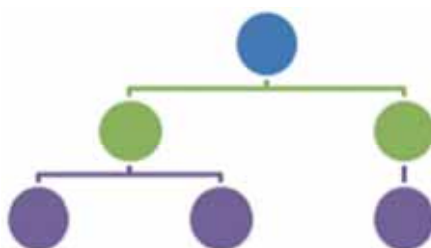
Group structure

In this section, the character of the group will be described in terms of its structure and its use of companies.

We have already touched upon the subject of structure when describing the recruitment of members and it is now time to elaborate on that topic a bit more. The six groups categorised as traditional organised crime that enters the internet are very hierarchic in their structure. The top of the pyramid consists of one or a few persons who run the organisation. They have the ultimate decision-making power and a complete picture of the activity of the group.

Underneath the top level are the middlemen. There can be multiple levels of middlemen, higher and lower in rank. They are usually not as involved in the entire activity as the leaders and their participation is instead focused on specific areas. Examples are also evident of middlemen not knowing who the leaders are or only knowing one of them, as in case 8, where the majority of the middlemen did not know who they were answering to because of the usage of aliases, no face-to-face communication and all communication going through other middlemen to the top.

Figure 6: Hierarchic group structure



Source: Presentation by the author

At the bottom of the pyramid are the people who can be described as foot soldiers. They can be seen to have very specific tasks, are not paid very well and are usually exposed to a higher risk of being discovered. This section includes mules in various forms; this can either be a question of putting one's bank accounts, addresses and names at the organisation's disposition or it may involve running small errands such as collecting or sending mail at the post office. For example, in case K18, the investigation identified 18 separate foot soldiers with tasks such as those of mules or collecting or sending mail at the post office. The vast number of individuals was necessary in order not to draw any suspicion to their activity and the payment they got never exceeded 50 Euro per errand and was usually no more than 10–20 Euro per errand.

As seen, the six organisations studied are run very similar to a business structure with different middle managers and areas of responsibility. In some cases the leaders referred to themselves as 'the board of directors', they sent out

weekly newsletters to all the 'employees' and they had proper payroll administration with salaries being disbursed once a month, on the same date as in the law-abiding world.

We can also see that the organisations included in our study not only work as a business, but also constitute and operate legal businesses. This phenomenon will be described further in the next section. Even if the smaller groups in our study, sometimes consisting of only four persons, are not as detailed as described above, the same hierarchic structure is present. Furthermore, the composition of these groups is rather stable with no major changes over time and especially not in the top region of the pyramid. One explanation for the stability could be the use of threats of violence that is seen in the cases, both within the group and in their external relations. This can be exemplified by case K16 where the leader was charged for attempted murder and aggression. Or case K10 where threats and harassments are present. It is mostly a question of rhetoric within the group, where they talk about all the things they could do. However, even if it is mostly talking, the result is a strengthening of the organisation, and of individual confidence and loyalty.

The use of companies

As mentioned in the previous section, the organisations sometimes operate within their own legal businesses. In our case study, two ways of using wholly owned companies are evident. The first example is that the illegal activity constitutes a small part and is hidden within an otherwise legal business. This means that, for example, certain revenues generated from illegal activities are not accounted for and are either used within the company for undeclared labour or taken directly by the owner as a profit without tax, as seen in case K16. It can also be as in case K17, where a group were involved in both illicit and licit gambling. The illegal profit was accounted for as part of the legal income from the licit gambling and the only way for an accountant to see that it was illegal money was to be active in their day-to-day activity.

The other method seen in the cases is that the suspects started companies to facilitate necessary procedures in the criminal activity. This includes field-specific companies for easier and less suspicious imports of particular items, e.g. where a group started a plate work company to import balers used to manufacture drugs. It can also be as in case K9 where they started companies in order to conclude contracts with other companies that offer services needed, e.g. online payment solutions, domain sites and processors in order for the organisation to construct and operate online pharmacies with online payment methods. Moreover, they also use other legal businesses and services not owned by the criminal group such as banks, post offices, currency exchange offices and other money transfer services outside the banking world.

Motive

All six groups in this category of Cyber-OC are driven by economic gains. On a general level, the groups and the group members in high positions are solely profit-driven and the economic aspect is the primary reason. On the individual level of the periphery members, the preliminary motive is to earn money, however, a threat or a need might be the underlying cause. For example, a common reason for many of the suspects in this study is that they have debts or are falsely accused of having debts to the group, which they are forced to pay off by performing specific tasks or being a mule. For example, in one case, one person had a debt to the leaders of the organisation and was thus forced to collect packages at the post office for the organisation's cause. Every visit to the post office was worth a specific amount of money. Hence, the person needed to continue collecting the post until the debt was no more.

4.1.2 Organised crime that develops in an internet environment

Background

Moving on to the next type of Cyber-OC, the person behind organised crime that develops in an internet environment is equally hard to generalise. Just as the previous section discussed the characteristics of the suspects in terms of age, occupation and previous convictions, this will once again provide the basis for the coming section.

These nine groups are also relatively homogeneous in terms of age. What differentiates them from the groups described in the previous section is that the gap between the oldest and youngest groups is not as wide; the overall age is thus more homogeneous. Even if the majority of the suspects studied are unemployed, there are more students involved in these cases of organised crime that develops in an internet environment than in the cases of traditional organised crime that enters the internet. Thus, several persons are involved in a daily activity, even if it does not generate any income. This might be due to the fact of the suspects being younger or that students have a lower income and are looking for ways to earn money. The cases also show that there are far more people whose job or studies are within the area of ICT. Some of them can be called experts and some have more mainstream knowledge. They include everything from network technicians and software engineers to consultants within domain solutions, and web developers.

Regarding previous convictions, there are two occurrences visible in our study. Those with previous convictions have either had sentences for petty offences such as traffic violations and the possession of drugs, or they have a background in financial crime, mostly involving different types of fraud. The

economic crime was not necessarily committed in an organised form and there is no visible evidence of the suspects having been involved in traditional organised crime prior to this.

Recruitment

When it comes to the recruitment process of these nine groups, they mainly look to their environment for siblings, friends and acquaintances. The more central a position the recruited person is to have, the closer a friend he would have to be. There are also two other types of recruitment in our study that are, if not as common, at least not foreign. Firstly, there are online meeting points. It could be that the group is advertising for special knowledge that they need but it could also be that they meet people online that they become friends with, such as in case K3. Just as there are websites, chat rooms and online groups for fans of a specific football team and discussion forums for motor sport, there are online communities e.g. for people involved in carding and hacking. These websites enabled the group to exchange services, advice and warnings with like-minded people and friendship developed between the group and another online member who was then recruited. Even if they had never met before, our case shows that they consider themselves as friends and the person is thus trusted to be a part of the organisation. The second online recruitment process evident in our study is not a full recruitment and concerns Crime-as-a-Service. This means that they advertise or contact advertisers to buy services, software or information. The person is thus not recruited but their knowledge is. This practice will be further explained in the later section regarding the preparations of the group.

Initiation

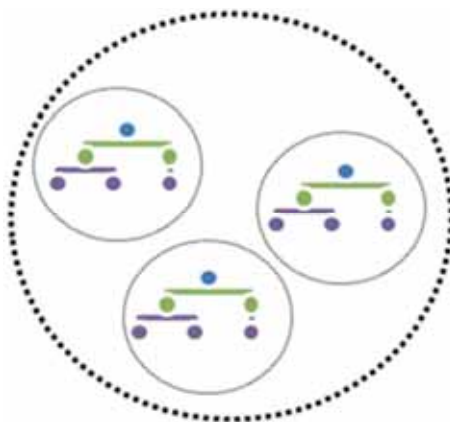
Lastly, the initiation of the criminal activity and the group in these nine cases differs from the previously described Cyber-OC category. In these cases, the idea of the crime often predates the group. It is thus usually one or a few persons who come up with an idea of how to make money in an illegal way who then recruit the people needed. As an example, case K4 shows how one person with knowledge of how to use wireless remote consoles to remotely control computers got the idea of using this knowledge to transfer money from the bank's account for his own use. He thereafter recruited a) people he could trust to build and test the console with, b) people who could break into a bank and install the console, c) a person who knew how to operate the bank's system, i. e. a former employee, and d) a mule.

Group structure

It is not only the sequence of events in initiating criminal activity that varies. There is also a structural difference between the studied groups involved in organised crime that develops in an internet environment and the groups in

our study categorised as committing traditional organised crime in an internet environment. As described above, the latter six groups are very hierarchic. The former groups are also hierarchic but the organisation usually consists of networks of clusters or spheres with inner hierarchic structures. This means that one organisation can actually consist of several smaller organisations or groups that cooperate for either the same purpose or different purposes and that are dependent on each other's activity. The inner structure is not necessarily as strictly hierarchic as within the traditional organised groups. Instead, the boundaries between the different levels are more 'floating'. The clusters or spheres can also be relatively autonomous in relation to the network. They have no insight into the other groups in terms of activity and members, they can work within multiple networks simultaneously and they can decide for themselves whether they want to continue to contribute to the cooperation or not.

Figure 7: Network of clusters



Source: Presentation by the author

However, these large networks of groups are of course not the only way groups involved in organised crime that develops in an internet environment operate. There are also several examples in our study of smaller groups, structured as clusters or spheres with an inner hierarchy as described above, that operate on their own. The keyword when describing the groups included in our study, whether it is in terms of inner structure or the overall organisation of the network, is 'floating'. This can be exemplified by case K7, where the four sentenced individuals never committed one act all together but instead every act was committed by different and various constellations of the four persons.

This type of structure has a lack of 'group spirit', which also contributes to an internal distrust of each other. This is evident within the individual clusters, where the studied suspects expressed a constant awareness and assumption of being deceived by group members. It could either be that someone takes a larger part of the profit than stated or that some might withhold valuable information for personal gain. This sentiment is also apparent between the clusters or spheres, where the different groups harbour some levels of distrust towards each other. Our data shows that owing to the anonymity, they cannot be sure to whom they are giving their contribution, if they will get the correct compensation or if they will be betrayed to the police if caught. The anonymity also strengthens the power of threats since one is not sure who the others are. Threats can therefore be genuine but also exaggerated and empty statements. Likewise, at the same time as the anonymity strengthens this power, it can also weaken it. This is especially the case in relation to the larger geographical distances between the involved parties. A decreased significance of intimidation tactics also affects the reason as to why one stays a part of the network and performs one's assignment to the full. If the traditional OC groups under study that enter the internet strengthen their members' loyalty through threats and violence, these members or clusters are shown to pursue this for the sake of their reputation in order to create a 'criminal CV', since the structure is as 'floating' as it is and new possibilities for cooperation are always down the line. The members are therefore dependent on the reputation of their skills and performance. If they do not perform what is agreed, their on-line reputation can be spread globally and rapidly and result in no more arrangements.

The use of companies

As said, these nine groups have been shown to sometimes be dependent on other people's information and knowledge but they can also be dependent on companies. The usage of wholly owned companies was described in relation to the previous category of Cyber-OC. This feature is not at all as common in this category. Instead, legal companies and services independent of the group are used. Quite a few of the cases in this study were dependent on special equipment. This could either be technical components purchased in a regular store that they constructed devices out of or plastic cards, printers and magnetic equipment for the production of counterfeit cards. However, the most common use of companies within this studied group is as marketing channels and this specific practice will be elaborated on further in relation to the groups' *modus operandi*.

Motive

Two kinds of motive appear in this group of nine studied organisations. The first one is economic and the criminal activity may, just as in the previous

Cyber-OC category, solely be pursued in the interest of profit or because of debts. The second motive that is present has been termed an ideological motive. This means that the people are committing acts based on a general belief, e.g. that information should be free or that their targets, usually institutions of the state apparatus, are committing wrongdoings. It could also be to draw attention to a problem, to make a statement or to show off one's skills. These two motives, economic and ideological, usually interact with each other. For example, as seen in cases K3, K7 and K18, there are one or several hackers that see the hacking as a challenge to overcome or as a way to show a gap in a security system. They are therefore primarily ideologically driven but when they have obtained the information needed, they will also sell it to gain money and they therefore sold it to the groups studied in the cases. The economic motive is therefore secondary. Then there are those who are only ideologically driven, who hack and hijack websites to spread information or post pictures for a specific cause. Several of the individuals in case K1 have themselves expressed that they were not economically driven, that they were solely involved in file sharing because of their beliefs that information should be free and available for everyone. However, when studying their organisation, one can see that they were actively selling advertisements on their websites to generate an income and based on the revenue they obtained from the activity, one might highly doubt that they did it only because of ideology. Hence, no cases in our study show an absence of economic incentives.

4.2 Activities and modi operandi in the field of Cyber-OC

In this section the crime types and modus operandi will be described within the two categories of Cyber-OC. The description of the modus operandi will be based on fixed points in order for it to be as structured and coherent as possible. The main features are crime type, ICT relevance, preparations, crime scene and marketing channels but other characteristics will also be highlighted.

4.2.1 Traditional organised crime that enters the internet

Type of crime

As the overall categorisation implies, the criminal activity that is described as traditional organised crime that enters the internet involves crime types that are usually referred to as traditional organised crime. This includes trafficking, drug smuggling, extortion, the sale of counterfeit goods and illicit gambling, often with financial crimes as a consequence of the preliminary activity, such as accounting fraud, benefit fraud and tax evasion. The ICT element

of the crime has contributed to the effectiveness of the offence but not changed its characteristics comprehensively. This will be described further in the coming section.

Modus operandi

The ICT relevance of the criminal activity has already been touched upon in the section above describing the type of crime committed within traditional organised crime that enters the internet. It is now time to develop this a bit further. As stated, the involvement of ICT in these six cases has contributed to the effectiveness of the offence but not changed its characteristics comprehensively. It is mostly a question of internet-assisted crime, if referring to our four categories in defining cybercrime. ICT has thus been used as a tool in order to gain advantages and it is replacing former procedures. This can take several different forms but three areas of conduct in which ICT is commonly used are identified within our study. Firstly, it is seen to mainly replace a more traditional form of communication. In relation to suppliers, buyers and victims, our cases show that this is mostly done through websites and crypto-markets where one can advertise and order products. This means that suspects involved in narcotic-related crimes can buy raw materials for their own production online and sell narcotics to other users online, as seen in cases K9, K10 and K19. For people involved in trafficking, such as in case K12, this means that the girls the organisation trafficked were advertised on websites instead of, or combined with, walking the streets. Another interesting situation, visible in one of our cases and that will be described in more detail further on, shows how online communities, such as dating sites, are used by organised groups to get in contact with persons with the intention of blackmailing them. This online contact space generates a broader audience for the crimes committed and ultimately global distribution and access.

However, the global and online channels of communication are not only used in the groups' external relations. There are also cases of groups in our study who mostly or only use online communication within the organisation as well. This has shown to ordinarily involve encrypted email and computers, information sent through apps or cloud services: services used to avoid detection or hinder evidence retrieval in case of a trial. In case K10, they did not only use the above-mentioned tools. They also created a regular email account that everyone in the group gained access to by knowing the password. They then wrote regular (non-encrypted) emails to each other but instead of sending them, they saved them in the draft box. In that way, other members in the group could read the message and then erase it, without leaving any trace of its existence and without any possibility for the police to retrieve a copy of it from the email company. It is thus not only the groups' external audience that can be globally scattered but also the groups themselves.

Secondly, the six groups encountered are economically driven. In order for them to retrieve their criminal profit, online channels of payments are often used. Cryptocurrencies, online banking and payment methods with higher anonymity are replacing traditional cash management in a physical environment with personal encounters as well as regular bank accounts and bank transfers, which are easy to track. This is also increasing the anonymity of the offenders. Out of the six cases in the category of organised crime that enters the internet, all six used online payment methods. Only one case, K12 concerning trafficking, did not use online solutions as the main channel of receiving their profit.

The last example of ICT as a tool is in relation to control and can be exemplified by two cases of illegal gambling included in our study. These organisations sublet slot machines that, through an internet connection and without valid authorisation, have illegal usages. Through installed software, the groups were able to control the exact revenues, expenditures, percentages, etc. of the slot machines. This not only facilitates administration but also reduces the risk of being deceived by the people renting it.

The new channels of communication, payment and control are thus making the six studied criminal activities more effective through an increased area of operation and a reduced time input. In the end this also contributes to a maximisation of profit.

Regarding the preparation of the crime, our study shows that this mainly includes recruitment. When focusing on the structure of the six groups involved in traditional organised crime that enters the internet, it was described as being very hierarchic. The preparation and recruitment is centred on the periphery level of group members. This includes finding mules and strategically placed persons, either in cities or in positions needed. One case, K9, included establishing contacts with a supplier and sending a member to meet the supplier and to scout the range of products. In the same case, another member settled abroad to take care of shipping and the group recruited a doctor in an advisory function. Another example is K13, which consisted of a group of boys pretending to be girls online who recruited girls to provide their pictures. There is also a group included in our study that was involved in trafficking who recruited girls for prostitution or persons to work as their drivers.

The physical place and cyberspace are relatively intertwined when it comes to the crime scene of the six cases included in this category of Cyber-OC. However, even if both places are integrated, they are quite easy to separate and define. The crime is usually initiated in an IT environment to be completed at a physical place. As an example, organised groups included in our study sell narcotics and have customers who order online. The product is then produced, packed and shipped to the customer's address. These are all activ-

ities connected to a physical environment. The same applies to trafficking women for sexual exploitation; the customers come into contact with the girls through online ads, where they specify the time and place. The crime is then finalised when the girls meet up with the customers. Even if this is how the majority of the cases proceed, there are of course exceptions, as exemplified next.

In one case in our study, K13, the suspects got into contact with their targets online and met them once under illegal circumstances to gain a hold over them, in order later to subject them to extortion via email. Thus, the crime was initiated and completed online with a physical meeting point in between. Another exception is in relation to the previous statement about physical space and cyberspace being easy to separate. It concerns the cases of illegal gambling, where slot machines connected to the internet were used for gambling. The gambler needs the machine to access the game but the game itself is solely based online. Hence, the physical and cyber-related scenes of the crime are intertwined to a higher degree.

Discussing the crime scene in relation to the cases categorised as traditional organised crime that enters the internet is closely tied up with the discussion of the six groups' marketing channels. The purpose of marketing channels in these six cases of Cyber-OC is to come into contact with customers or victims. This is mainly done through self-administered websites or online forums, as mentioned before in the examples of ordering drugs online or calling for a prostitute through an online advertisement. There are also some examples of physical stations, such as the cases involving slot machines.

Target and profit of crime

The criminal activity of the six groups studied is mainly directed towards customers or persons where the target and the group have a bidirectional relationship. This means that the contact is based on the initiative of both parties. There are some more obvious cases of this, such as the above-described online-based sale of drugs and prostitution as well as the illegal gambling machines. They are all reliant on customers or persons responding to their offers with a request or intention to use their product. There are also less obvious set-ups, for example case K13, where a group who claimed to be underage girls came into contact with older men online and decided to meet up for sexual purposes, to later blackmail them. Even if they are not customers, the method is based on an active dialogue between both parties in which the men are willing to meet the 'girl'.

Evident in our study and in the six cases of traditional organised crime that enters the internet is that the profit of the crime is usually handled within the legal company or the group. It could be as illegal wages, legal wages, invest-

ments or external expenditure. The smaller groups, who do not have a clear business structure, often receive the profit back to the group to be divided according to a set percentage arrangement. Furthermore, there are two ways that these six groups receive the profit back into the organisation. It is either based on online transactions and mules who put their bank account at the group's disposal. This can include both 'regular' currencies and cryptocurrencies. Or it is cash-based, which makes currency exchange offices and companies providing money transfer outside the banking system an important and frequent channel.

4.2.2 Organised crime that develops in an internet environment

Type of crime

As the title of this category suggests, the crime types committed are dependent on ICT. These can be completely new crimes, which do not have a predecessor, e.g. computer hacking. But they can also be offences that have a traditional mode but when using ICT the performance and scope of the crime changes comprehensively. For example, fraud has been committed in various forms throughout history but when criminal groups gain access to bank accounts or credit card information through hacking databases, skimming, phishing or Trojans, not only is the method dependent on ICT, they will also maximise the reach and profit of the offence in a way not possible by traditional means. Another example is file sharing and violating copyright law, which could be seen to have a traditional prototype in the sale of counterfeit goods. By digitising the access, the information is given a global reach and the economic loss of the plaintiff company is dramatically larger.

Modus operandi

The studied cases in this category are rather different from the other category's cases in their relation to ICT. As already mentioned in the previous section, these types of crimes are dependent on ICT. When talking about the ICT connection in the category of traditional organised crime that enters the internet, it has been discussed in terms of the internet being a tool, where the internet came to replace a specific part of the procedure. In these nine cases, ICT is an integrated part of the entire modus operandi. Most of the criminal activity is committed through or reliant on computer integrity crimes. Examples from our cases show that it could be that the group bought credit card information from a hacker to commit fraud; it could be that the group takes over a computer and controls it remotely to transfer large amounts of money; or it could be that the group has gained access to online poker accounts of hundreds of persons through a hacked database to deliberately cause them to lose against the group members. Some of these crimes involve cryptomarkets,

where the information is bought. Even if these crimes are classified as computer integrity crimes and sometimes include cryptomarkets, they are often also internet-assisted. However, the part where they use the internet as a tool has been shown to often constitute a secondary part of the crime that could have been carried out without the use of the internet. For example, when the credit card information is bought, the group could – instead of buying things online – manufacture a false credit card to go to the stores and buy items. They could also, instead of selling the item online, sell it at a market. Furthermore, there is another side to these crimes. There are cases in our study defined as internet-assisted crimes that are not computer integrity crimes but still equally dependent on ICT, e.g. K1 concerning file sharing and K14 regarding violations of copyright law. Here, ICT is used as a tool in every single step of the modus operandi, making it more or less impossible to commit the act without the internet.

Regarding the preparations of the crime, this category is quite similar to the previous one regarding recruitment of the right persons, such as mules. However, what distinguishes these nine cases is the recruitment of services and construction material. These groups are not always experts within the field of computers themselves and they are therefore dependent on external knowledge. Three main methods of obtaining this knowledge are evident in our data and will be explained and exemplified below. Sometimes it is necessary to buy information from an external person, e.g. credit card information. This is usually done through cryptomarkets, where the seller and buyer come into contact for this specific transaction. Traces of such activity can be seen in cases K7, K8 and K18, showing how necessary information is obtained without recruiting a person. Sometimes the group establishes cooperation over an extended period of time. This knowledge is not necessarily only in relation to ICT. For example, in case K3, the group established cooperation with both a person who could counterfeit ID documents and a software developer. These persons were not a part of the group but they had cooperation and personal interaction over a long period of time. One might say that even if the experts were not a part of the group, they were semi-recruited. Lastly, the group can fully recruit a person with the knowledge desired, for example a hacker. The groups were also described as distinguishing themselves by constructing material. This could either be to create software programs or Trojans, skimming equipment or remote-control devices that were to be assembled on an object, or it could be to manufacture counterfeit credit cards. Other types of preparations that are common to both categories are clearly communicated rules of conduct, legal aspects taken into consideration and plans to conceal the crime and/or the profit of the crime.

As a continuation on the internet-based activity, the crime is usually committed in a pure internet environment, i. e. the physical environment is not an

integrated factor. There are cases in which the crime is solely committed through cyber instruments, for example file sharing, computer hacking and internet fraud. In these cases, all phases of the *modus operandi* are committed within an ICT environment. Case K1 concerning file sharing can be taken as an example and was committed through three cyber-based steps. Firstly, the material or information was gained, digitalised if not already and packaged in a desired format. It was then uploaded to an online platform for public access, to be later downloaded to individual persons' computers for personal use. All three steps have cyberspace as their crime scene and even if there are personal acts behind these steps, that person's physical position is irrelevant for the act. There are, however, cases in our study that still have a physical element to them, for example the production of counterfeit credit cards or collecting ordered items from the post office. These elements are, nevertheless, not the central point of the criminal activity.

The last section of the *modus operandi* of groups involved in organised crime that develops in an internet environment concerns marketing channels. The main purpose of marketing channels is in these cases to retrieve the profit of the crime. There are two features visible in the study on how this is done. Firstly, it could be through single transactions. This means that the transaction is only made in one step. It could either be that the group transfers money from the illegally accessed account to a network of mules. Or it could be as in one of our cases, where a group gained access to online poker accounts and deliberately lost against themselves. However, it could also be done through double transactions; here the profit is transferred in multiple steps. This can be exemplified by several cases in this study concerning online fraud where the groups bought items with a stolen credit card to then sell the items on online second-hand markets or online auctions and through this procedure gain money. There are also two less prevalent characteristics for retrieving the profit. One is that the groups do not use any mules or middle steps at all. Instead they transfer the money straight to their account. The second feature is through wholly owned websites, where revenues for advertising bring in the economic profit, as seen in case K1.

Target and profit of crime

The type of criminal activity that these nine cases are engaged in mainly targets private individuals. It is usually a case of gaining illegal access to something belonging to a person: e-legitimation and bank accounts for fraudulent purposes, computers through ransomware or Trojan attacks, etc. There are also signs of the studied groups targeting companies and sometimes authorities as well, especially in cases of ransomware or hacking attacks to retrieve information of a specific sort. The purpose of the crime is the same irrespective of whom they are targeting. The reason there is a growing focus on com-

panies and authorities is because they handle a larger amount of money and information than a private person. One attack can therefore generate a larger yield of the crime. What private persons, companies and authorities have in common in relation to the criminal group, and what differentiates this group of Cyber-OC from the other, is that the contact is unilateral. The study shows that the relationships between these nine groups and their targets are not dependent on or characterised by mutual interest. The groups are not involved in an environment of illegal goods and services. Instead, their criminal culture consists of gaining illegal access. The targets in these cases can therefore be described as victims. There are of course exceptions as well and there are cases in which the criminal activity is dependent on a bilateral relationship, e.g. in file sharing.

The groups' processes in retrieving their profit are described in relation to marketing channels. This section will therefore mainly focus on where the studied groups place their profit and how the money gets there. The two main destinations visible are their own bank accounts and private bank accounts abroad, belonging to them or other persons. Besides transactions within and between different banks, other transaction services and currency exchange offices are used. Owing to the alternative transaction services as well as the simplified and more user-friendly systems within banks, the money reaches foreign accounts faster and further away.

4.3 External cooperation in the field of Cyber-OC

There are two kinds of cooperation, voluntary and forced. The following sections will explain the different types under the headings of contacts and unlawful influence. These areas have already been touched upon when describing the structure and recruitment process of the criminal groups. This will not only be developed further but, unlike the previous sections which also included the internal collaboration, this section will solely focus on the groups' external cooperation.

4.3.1 Traditional organised crime that enters the internet

Contacts

Within these six groups of Cyber-OC, little cooperation is seen. The studied groups are fairly autonomous and the competence needed is recruited. However, there are two kinds of cooperation visible, even if this occurrence is less prevalent. The first one concerns practice i.e. it involves some kind of service. There are two cases in the groups studied that have some kind of coop-

eration with different types of gangs. So far, only the contact in itself is evident and not them using the cooperation in any way. It is therefore not exactly certain what form the cooperation takes but it seems that they trade violence for money. This is not only a specific sum for a specific act but the study also shows that one of these groups gave the family member of a gang member a financial contribution while the gang member served time in prison, in order to 'keep the gang happy'. There is also a group that has some sort of collaboration with a lawyer. Once again, evidence is only found on the contact itself, not on the actual cooperation and it is therefore not completely certain what it entails other than the lawyer getting money on the side to break the obligation of professional secrecy when dealing with their case, etc.

The other form of cooperation is in relation to knowledge. In our study, the group in case K12 is seen to cooperate with another group with similar arrangements to gain new knowledge. In this case, members of the first group went to visit the other group and accompanied them when they set up and managed skimming equipment. This would complement the first group's preliminary crime, trafficking. There is however no information on the outline of the cooperation and what the first group contributed with.

The most common way of initiating these kinds of cooperation in our study is through face-to-face contact i.e. a member of the group is already familiar with the cooperation partner. As an example, the lawyer who had cooperation with the group in case K10 was previously involved in criminal activity with some members of the group and started to study law while serving his sentence.

Unlawful influence

As said, there is no evidence in our study of threat, violence or other forms of unlawful influence being realised in practice but only of them being mentioned in conversations. Since it is merely a question of internal rhetoric, as mentioned in the section on the groups' structure, it might not be as serious as it sounds and instead used as a tactic of intimidation and to strengthen the group. Either way, it was a question of both punishing and threatening group members as well as external parties. However, there are no signs of the groups planning to direct these actions towards civil servants or parts of the legal system.

4.3.2 Organised crime that develops in an internet environment

Contacts

The cases of organised crime that develops in an internet environment included in our study involve a considerable amount of outsourcing, and

Crime-as-a-Service exists to a great extent. This influences the scope of cooperation and three different types of collaboration and contact relationships have been identified.

The first one concerns contacts as distinctive business relations. It could either be in relation to law-abiding businesses e.g. the group's company being approached by a law-abiding company that wants to sell and manage online advertisements on the group's website, as seen in case K1. It could also be business-like relationships between private individuals, where the group buys services or programs from a third party. This includes everything from buying databases of information, software, or services that maintain the technical infrastructure, to distinct services such as manipulating documents, cracking passwords, sorting the content of the databases and preparing lists of information for the group. The latter scenario is the most common one in our study and can be seen in the majority of the nine cases of organised crime that develops in an internet environment. In both situations, contact is often initiated online through specific forums and trust is commonly established through a 'product sample' that the seller sends the group to test free of charge.

The second type of cooperation visible is through online forums and does not have the business character about it. Instead, 'experts' and active practitioners meet at various forums to discuss different techniques, giving advice and warnings. In case K3, this was done in relation to hacking, carding, skimming, etc. and can be likened to friends who help each other without requiring anything in return.

Lastly, there are also a few examples in the study of the criminal groups having contact with traditional gangs. The criminal group is either currently part of the gang or it has been part of it. In the first example, there is no information on what the relations are or how the structure is divided up. The only information obtained is that the gang is known by the police, mainly owing to violent incidents and credit card frauds. In the second example, there is a person from a gang who gives 'permission' concerning who is allowed to operate within the crime type in the city and which areas belong to different groups.

Unlawful influence

Unlawful influence could possibly be present and, if so, it involves targeting company employees in order to recruit them as insiders. This information was collected from the interviews and is discussed as potential scenarios without any concrete proof to back it up. No signs of this were evident in the cases, either.

4.4 Summary suspects, groups, modi operandi and cooperation

The following chart summarises the distinctive features of the fifteen cases studied within the two different categories.

Table 5: Summary of group characteristics

Characteristics	Traditional organised crime that enters the internet	Organised crime that develops in an internet environment
Background	older, employed, no criminal background	younger, unemployed, criminal background
Recruitment	family, friends, acquaintances, social circle	social circle, online ads, online forums
Initiation	group → idea of ICT crime	idea of ICT crime → group
Group structure	hierarchic, company structure, stable, threats	network of clusters with inner hierarchies, distrust, threats and reputation
The use of companies	own companies and legitimate businesses as an integrated part of modus operandi, banks	other businesses for equipment, services and marketing channels
Motive	economic	economic, ideological
Type of crime	traditional crime	ICT-dependent crimes
Modus operandi	internet-assisted crime	computer integrity crime, internet-assisted crime
Target of crime	customers, bidirectional relationship	victim, private individuals, companies
Profit of crime	handled within company structures and organisation	own bank accounts, private bank accounts abroad
Contacts	fairly autonomous	considerably outsourced, Crime-as-a-Service
Unlawful influence	very weak tendencies	very weak tendencies

Source: Presentation by the author

4.5 Damage of Cyber-OC

4.5.1 Traditional organised crime that enters the internet

There are four relatively strong features within the six groups of traditional organised crime that enters the internet and the damage that their activity causes.

The first feature is economic damage: people are deprived of money. The first and clearest example is in relation to blackmailing where people are forced to transfer private money to criminal organisations, usually quite large sums. The second example is in relation to the black economy. The sale of illegal goods, such as counterfeit furniture, medicines and drugs, boosts the black economy and leads to economic losses for law-abiding companies.

The second aspect concerns health. When counterfeit medicine, drugs and stimulants are sold, the customers' health is at risk. We have seen several different variables during our case study that affect the safety of the customer. First of all, the preparation sold may not in fact be the declared substance. It could either contain a small variation of the original substance or it could be something completely different. Secondly, the preparations sold on the dark market are usually chemically assembled under conditions that do not meet the required clinical settings. These two examples, with their internal variations, on their own or combined, may give rise to undesirable side effects, incorrect medication intake and sometimes life-threatening conditions.

The third feature begins where the second tendency ends and regards distrust in various senses online. This can be distrust as a reaction to criminal organisations that purport to be legal online pharmacies or organisations that claim they are selling legal drugs and preparations. It can be distrust towards online dating sites or social forums: is everyone who they say they are? It can also be an overall cynicism towards the internet owing to previous experiences concerning misuse of online trust. This is also strongly linked to a general renunciation of online services, which might reduce online commerce and ultimately result in a decline in the economy.

The last aspect can cause damage to both the victim and people within the criminal organisation through social vulnerability and/or exclusion. Women subjected to online prostitution and mules who are exploited and exposed to the risk of being detected are examples of positions within the groups that can cause social vulnerability for the people involved. They can be deceived out of money, put in financial difficulties and risk a prison sentence that would affect their future opportunities to return to a law-abiding life while simultaneously giving them a bad reputation. In relation to the victim and blackmailing, as an example, they are not only put in financial difficulty but

the hold that the offender has on the victim might be of the sort that would cause social exclusion if revealed.

4.5.2 Organised crime that develops in an internet environment

Three types of damage are visible within the nine cases of organised crime that develops in an internet environment. Some tendencies emerge of the same kind as the above-mentioned, however, owing to the differences in *modus operandi*, the damage has different characteristics.

The first type of damage is economic. Just as in the previous category, this economic damage can be exemplified in two ways. The first division is, once again, in relation to the economic loss of private individuals. When credit cards are skimmed, phished or when ransomware attacks are carried out, money belonging to private people is transferred to criminal organisations. The victims are usually reimbursed by their bank or by other means. The banks are thus economically affected and in the long run also the customers of the bank. The second division is linked to the latter example: the economic loss for companies. This includes banks, as described above. It also includes companies that have the actual copyright and lose revenues owing to e.g. file sharing, and companies exposed to ransomware attacks.

The second type of damage is access to sensitive information. This includes credit card information, passwords, protected addresses and personal data, etc. Through various forms of computer integrity crimes, databases are accessed and access is gained to sensitive information. The data could also be generated through computer-related crimes such as skimming or phishing. Sensitive data like this can in turn lead to additional damage such as identity theft, economic losses, insecurity and distrust.

This brings us to the third type of damage: distrust, which can in turn be divided into two different types. It can firstly concern undermined confidence towards civil functions and their systems. This is mainly a consequence of e.g. skimming and phishing, and scepticism is directed towards cash dispensers, card payment terminals, banks, online banking and online services offered by authorities. The second type of distrust concerns a general distrust towards the internet. This includes a loss of trust in online payment systems, website security, social forums, online second-hand markets, etc., which in turn, amongst other things, leads to damage number one: the economic loss of companies.

4.6 Criminal investigation of Cyber-OC

4.6.1 How cases come to the attention of law enforcement

We will firstly explain the different ways a case of Cyber-OC can come to the attention of the police. We will then describe how investigations are allocated to the different investigation units and prosecutors.

Victims

There are five circumstances visible in our data collection regarding how cases of Cyber-OC have been reported to or by the police. The first and what seems to be the most common way is that the victim of the crime reports it. It can be through the police report system online, through a phone call to the police or through a visit to a police station. This procedure appears to be more common amongst private persons that have been a victim of a crime than amongst companies or authorities in the same position.

Letter

The latter group, companies and authorities, seems more prone to report a crime through a letter. In these cases, a representative of the affected party sends a letter stating what happened straight to the police, who file a report, or to the Swedish Prosecution Authority, who report it to the police.

Intelligence

A report can also be a product of the police's intelligence work. This is the case when the police have, at an earlier stage, worked against a phenomenon in general and after some time found enough evidence to say that it is likely that a crime has been committed. They can then file a report themselves and initiate a formal criminal pre-trial procedure.

Spin-off

The fourth way is similar to the above-mentioned example, where information about the crime is well known before the report is filed. This is initiated through international legal aid where a Swedish investigation unit is engaged in providing help and information to a police investigation conducted abroad. During this collaboration the Swedish unit might discover that the crime also has victims or a crime scene in Sweden and they will then file a Swedish report.

Multi-agency

Lastly, a case can also come to the police from another law enforcement authority that is pursuing its own investigations. This is usually the case when

the other authority believes the police will have greater success in the investigation or when cross-authority collaborations are established.

When a crime has been reported, a unit needs to be allocated the investigation. This process is rather simple and consists of two general steps. The first is identifying where the crime has been committed and signs that indicate the geographical region responsible. After that, the case is classified to be either a 'pure' ICT crime or a crime with ICT influences. A 'pure' ICT crime is in general a case of computer hacking, a so-called computer integrity crime, where the crime is directed towards a computer. A crime with ICT influences, on the other hand, can be either a case of computer content crime or a computer-assisted crime. Crimes classified as 'pure' ICT crimes are assigned to an investigation unit specialised in computer hacking. Crimes with ICT influences are identified by their crime classification e.g. fraud, trafficking or drug offence, and then assigned to the investigation unit specialised in that crime type.

Whether the investigation is led by a prosecutor or the police, a prosecutor will be assigned the case at some point. Just as there is a division and specialisation of investigation units, there is a division amongst prosecutors as well.

4.6.2 Investigation instruments, methods and strategies

When it comes to investigation instruments and strategies, three general opinions are expressed.

Up-to-date technology

The first one is that it is not a specific computer program, technical tool or instrument that is important. Instead, what seems to be the key factor is that the investigators are constantly updated on the latest information about methods of technology and that this technology is coherent and available for everyone who works within the field.

'The technology is important, we must have a better national system, so that the work one has is facilitated, that we have a consistency, I mean that it is invested in, so that one gets the opportunity to work effectively and with systems that everyone can work with.' (Interview 4)

The quote above is connected with technical methods used by the police for securing evidence, e.g. mirror imaging, which is based on generating an identical copy of the original hard drive. Literature regarding digital evidence highlights this method and its loopholes, which can lead to information not being secured. At the same time, the literature also shows its role as a cost driver owing to the allocation of storage space and time spent (Kronqvist 2013: 116).

However, the need for up-to-date technical devices is not unique for high-tech cybercrimes. In fact, an analysis of the suspect's computer and mobile devices can now be considered a routine procedure, at least when it comes to more serious crimes (Kronqvist 2013: 120).

A quick initiation

The second strategy that seems to be a factor in success is a quick initiation of the investigation. This aspect is strongly connected to the Data Retention Directive, which legally binds companies, broadband providers for example, to store electronic information for six months before it can be deleted. Literature has shown this data to be key information in Cyber-OC investigations and will be discussed further in sections 4.6.4 and 4.6.7 (Kronqvist 2013: 55–86). Sometimes this information is stored by a company abroad and mutual judicial assistance is needed, which increases the importance of time even more.

If the investigations are not initiated as quickly as possible, the risk of evidence being deleted before the police can secure it is greatly increased. This problem can be found in a number of our cases, where the investigators could see indications of the criminal activity being much vaster than what they could secure evidence for (K3, K7, K8, K18).

'When I started here [...] there were piles and piles of cases, and I sat here for fourteen days, looking through them all, and in almost all the cases we had passed the six-month limit and could not track them. It is tragic, but that is what we have changed now with the new process of cases, which allows one to quickly start the investigation. If one can see ideas or investigational leads, one can take care of that right away, and then we have a foot in the door and we can continue.' (Interview 5)

Cooperation

The third investigation method that is highlighted in our data collection concerns cooperation. The collaboration that is perceived as successful entails international actors, internal colleagues and the private and public sector.

'Once again, collaboration, that is when we see progress [...] it is very clearly shown in terms of results when we have good cooperation, then progress is shown, and it also applies to private actors, although the private and public sector have different procedures on how to handle incidents, collaboration is very important and it leads to the understanding of the whole picture.' (Interview 1&2)

What the cited person expresses can be exemplified by at least two of our reviewed cases concerning drug sales and illicit gambling. The investigations, which have been viewed as very successful cases, consisted of collaboration with other national law enforcement authorities, international colleagues within law enforcement and international private actors (K10, K17). The col-

laboration served two purposes. Firstly, it was needed to retrieve specific information located elsewhere and to decrypt it. Secondly, it also played a role in relation to more general strategic decisions and investigatory leads.

4.6.3 Special expertise

The subject of special expertise was brought up during the interviews in relation to various circumstances. This was with respect to specific cases, in terms of general Cyber-OC, from a prosecutor's point of view, from police experience, etc. Just as the previous section did not single out a specific technical tool or program but instead highlighted the importance of up-to-date and coherent technical help, the expertise needed was not discussed in terms of a specific kind of education but more in terms of general competence and characteristics.

Persistence

The general view of cyber-related crimes is that they are evidentially difficult to solve. This includes the entire process of securing evidence. Starting with the procedure of finding the evidence, the vast amount of information that ICT actions create requires investigators already in the initial phase to make strategic decisions and draw boundaries. After that, time-consuming work to find relevant information and obtain this in a legal way is necessary (Kronqvist 2013: 120-132).

This is reflected in our data where it is difficulties and bottlenecks in the process of obtaining evidence that seem to decrease the chances of solving a case, rather than the lack of evidence (K3, K7, K8, K9, K10, K13, K18, K19). As the following quote exemplifies, cyber-related crimes have evidential difficulties that affect the outcome of the investigations.

'We work on the cases as much as we can and we try to run them down as far as possible and then, when we cannot get any further, we close the case. That is what is the most mentally challenging part of our job, that we have so many cases that we cannot get anywhere with, but the guys here are really trying.'
(Interview 5)

It is thus not surprising that one of the main characteristics that the interviewees described as necessary is to be persistent (interview 3, interview 5, interview 6). As several of our cases show, the evidence is found in the details of the information (K7, K8, K16, K17). The amount of information, the early drawing of boundaries, the process of obtaining and finding relevant information, and later reviewing the details to find the evidence all require persistent work. In the end, data that seems to show the entire picture can always be investigated and enlarged on further. As the following quote exemplifies,

many of the cases in our data collection have been brought to trial thanks to investigators, forensic staff and prosecutors who kept searching for information even if they had been given the answer that nothing had been found.

‘You have to be stubborn [...] We might never have succeeded if it was not for a persistent forensic scientist at a fairly early stage of this investigation; he received information from an internet service provider that he was not satisfied with and continued to search for more information, which then led to the first raid.’ (Interview 6)

Knowledge in terms of ...

... experience and further education

In terms of more hands-on expertise, knowledge is highlighted in three specific areas and the first area is knowledge gained through experience and constant development. To solve cyber-related cases, knowledge of the field is important. Since the area of cybercrime is ever developing, this knowledge is mainly gained through past experience and current constant development. It is therefore important to have investigators who have been involved in cyber-related crimes for a while and are simultaneously aware of technical changes and continue to search for new information.

‘The knowledge is to a high degree empirically gained, it is not just a question of looking it up in a legal dictionary or reading some manual and then you know what to do. It is important to network [...], to spread the knowledge, both within the police but also amongst prosecutors.’ (Interview 6)

This is, as already stated, due to the ongoing development of ICT and how it can be used for criminal activities. As stated by Wall, the advantage of crimes depend on ICT is that the technology already exists to solve it, you just need to know how and what to use.¹⁰⁷ In order to keep up with new technology and new applications, constant development and training is necessary for the investigators and forensic scientists (Kronqvist 2013: 51). This is not only a line of reasoning from literature regarding crime and digital evidence, but it is also expressed by our interviewees, as exemplified below.

‘The key to good investigation is constant development of the people behind the investigation.’ (Interview 3)

Furthermore, the need for experience and further education is also connected to the lack of national guidelines for methodological cybercrime support and the lack of a common standard for forensic education, equipment and methodology, as described in chapter 4.1 (RPS 2014). Owing to the absence of na-

¹⁰⁷ At a seminar in Stockholm.

tional guidelines on how to investigate a cyber case in the best way, this information needs to be obtained through practice, as the following quote describes.

'It is actually an experience-based learning, more or less. We see trends when they appear and we try to find a method that we can use [...] and we use that method in the investigations and either we notice that it is successful, and if so we continue using that method, or we notice quite soon that no, it is not working.' (Interview 5)

Hence, owing to the developmental nature of the field together with an absence of national and common best practices, one is dependent on the investigators to carry out up-to-date and experience-based investigatory work.

... the ability to adapt

The second type of knowledge desirable is the ability to adapt: being aware of the need to adapt and knowing how to adapt. This is connected to the evidentially difficult character of cyber-related cases and takes up where the discussion regarding the importance of persistence leaves off. Since persistence and the continuous search for information are important, the investigators also need to know alternative ways of obtaining the information wanted. This is mainly connected with the process of retrieving the evidence in a legal way and its dependence on cooperation between the police, other countries and private actors.

For example, in one case they needed to prove that two people had had contact via an internet-based communication app. They could not *technically* retrieve the information from the people's phones and were therefore required to get the information from the company itself. This company was based in a country that they had not had good experience with in previous cooperation. If they ever got an answer to their request for legal aid, it was usually several months or even years after they sent it. However, they knew that they had to prove that these two persons had had contact and they were therefore looking for alternatives. The prosecutor had better experience with legal aid from another country where a popular social forum was based and during the interview with the aggrieved person it was revealed that the initial contact had been via that specific forum. It was possible to send the legal aid request to that country and the information needed was retrieved (interview 3).

It is thus important to try to reach the information in all possible ways, as one interviewee stated:

'So it is primarily all about the ability to adapt, I think, and to know what information is essential, and from there one can determine the possible ways of retrieving it.' (Interview 1&2)

... understanding the law and securing evidence

The third and last aspect of knowledge is to understand the law and to know how to apply it in practice, especially in relation to how to secure evidence. As previous publications emphasise, evidence gathering from the internet can often be technologically advanced and involve time-critical information. In addition, this procedure includes a legal framework that is anything but clear (Kronqvist 2013: 55). Our data articulates the same view or, as an interviewee explained:

‘The law is not designed for apps; one must therefore know how to apply the law to apps.’ (Interview 3)

This means that you have to understand what you can do. The laws are not written with cyber-related cases in mind, at least not the majority of them. The police and the prosecutors must therefore know how to translate and apply the law to a cyber environment.

The following reasoning is an example of how the act of information retrieval can cause the police and prosecutors problems in cyber-related crimes. The examples can be found in all our cases and are expressed in numerous interviews (interview 3, interview 5). Firstly, and in relation to understanding the law in general, one has to know the answer to the question ‘Where is the information?’ Is the information located on the mobile phone or in a cloud service that you can access from the mobile phone? This has a huge impact on how you can retrieve and save the information legally. The correct answer is that the information is located in a cloud service owned by a company. It is therefore very important to turn off the Wi-Fi access on the mobile phone or put it in aeroplane mode. When doing so, the information accessed through the mobile phone is no longer in a cloud service but located on the mobile phone itself.

In relation to the knowledge of how to secure evidence, in addition to the above-mentioned example, one needs to bear other aspects in mind. It is important to know that a cloud service enables multiple devices to be connected to each other. One can thus erase data on a device that has been seized through equipment that has not been seized as long as the seized device is connected to the internet. This is a second reason why it is important to remove the internet access.

This division based on the location of the information corresponds with the division of Stefan Kronqvist’s discussion of openly available information, which one is entitled to retrieve by oneself, and information not openly available to retrieve which one needs consent from the person owning the information or authorisation of coercive measures (Kronqvist 2013: 55).

It is also important to know when one should turn the device off in order to save the information and when one should keep the device on in order to secure the evidence. In one case in our study, the law enforcement agency in charge of the investigation made sure they made the raid at a time when they knew that the computers were on in order to bypass encryption software. After that, they needed to constantly move the mouse so that the computer would not go into a state of rest before the IT forensic staff came. A second scenario, in contrast to the first example, was described by an interviewee where the suspect, as soon as he realised there was a raid going on, pressed a button to erase everything on his computer. By pulling out the power cord, the resetting of the computer was interrupted and the evidence was not erased.

The recipe for success is thus, in summation, to have investigators who are persistent, who have worked within the field of cybercrime and who want to continuously learn more, who know what information is required and that one needs to adapt and look for alternative ways to retrieve it, and lastly, who understand the law in relation to cybercrimes and how to secure evidence.

4.6.4 Which information is difficult to uncover?

Information ...

Our analysis has shown four areas that, in relation to information, affect the level of difficulty in uncovering the evidence needed. These four areas are (1) information affected by the Data Retention Directive, (2) information accessed through international legal aid, (3) encrypted information and other anonymisation services and (4) the amount of information generated in cyber-related cases. Although they are four separate areas, they can often affect each other as well as work alongside one another.

... in relation to the Data Retention Directive

The first aspect of information difficult to uncover is information affected by the Data Retention Directive. As stated in section 4.6.2, an early initiation of the investigation is a key factor for a successful investigation. Since the Data Retention Directive only guarantees that certain information particularly important in Cyber-OC cases is saved for no more than six months, this key information can be lost for ever (ibid.). This includes internet connections with IP addresses, mobile phone locations via telecommunications masts, etc.

‘It is very time-critical in our cases. The Data Retention Directive is really great but it can be quite stingless in international cases. A network operator needs to save data traffic for six months and then they delete it, and six months passes by quickly when you begin to look into a case that you see has an international

connection, and then you have to contact that country and before they process it, six months has almost passed [...] and it is essential for our investigative function to be able to obtain information about who has had an IP number at a particular time [...] and if one misses the deadline, it usually leads to the closing of the investigation.’ (Interview 1&2)

... in relation to international legal aid

As already mentioned, legal assistance is important for various reasons. It could either be to understand the bigger picture of the case, in order to investigate and follow up on important leads or to retrieve key information from international companies and authorities.

However, legal aid is not exclusively a helpful element in an investigation. It can also have a restricting effect.

‘In Sweden, we have the privilege of reaching quite far in our investigations, but the cases that we investigate rarely only involve Sweden, Swedish citizens, people living in Sweden [...] and as soon as there is another country involved, our ability to successfully investigate decreases.’ (Interview 7)

What the interviewee expresses is found in a number of the analysed cases, many concerning fraud and the distribution of narcotics. In these cases, the requests mainly focused on bank accounts that belonged to potential victims and offenders, but the requests had not been answered (K7, K8, K10, K18, K19). Owing to the lack of response, it is written in the criminal pre-trial proceedings that several additional potential criminal acts remain unconfirmed as well as further potential offenders.

Of course, it is not always true that a request for legal aid results in a lack of response. The number of solved cases proves otherwise and helpful assistance is given. However, there is also a third outcome of a legal aid request: a delayed response. Some countries have such a long list of tasks that when they assist, their help is too late and the case is either already closed or the information has been deleted.

... in relation to encryption and anonymisation services

The third factor that makes information hard to uncover is encryption and other anonymisation services. This can in turn be divided into two separate problem areas: the complicated procedure of decrypting information and the lack of obligation on the part of private companies.

The first problem mainly concerns encryption located abroad and anonymisation services used by criminals. Legal aid is thus needed and when the time-consuming procedure of legal aid is added on to the time-consuming procedure of decryption, the investigation suffers. As one of the interviewees said:

‘One usually needs legal aid to decrypt an encrypted email [...] and as soon as we deal with encryption, the time starts ticking [...] Encryption is not difficult but it takes such a long time and you rarely have the time to wait for an email to be decrypted in order to get it into the preliminary investigation.’ (Interview 7)

This is exemplified in one of our cases where the legal aid and decryption process took almost two years (K10). The scope of the investigation was large and ongoing during the entire time, hence the possibility to wait for the decryption, which turned out to be key evidence. Another investigation, concerning a rather small case of narcotics, did not have the time to await the decryption and the suspects were brought to trial before all possible evidence could be included (K19).

The second problem concerns privately owned encryption and anonymisation services. The private sector has no obligation to disclose information to the police and the investigation therefore needs to be of the sort that search warrants or other coercive measures can be called for. This does, of course, take time and when the encrypted information is a subject of the Data Retention Directive, too long a waiting time can make the efforts futile.

... in relation to its vast amount

There are numerous aspects of investigatory work that need to be revisited when the evidence is in the form of information and there are vast amounts of it. As the criminal pre-trial proceedings of our cases indicate, an enormous amount of documentation is needed when crimes have been committed over the internet. This vast amount of information and documentation of the information require analytical resources on the part of the investigators and the process of going through all the material is highly time-consuming. In fact, it is more time-consuming than analysing evidence in traditional crimes, as one interviewee explained:

‘Another problem that is a real challenge and that we do not have in more traditional crimes is the amount of information; the amount of information is incredibly large. In a traditional case you will find some notes and bags that you retrieve traces from, it is a manageable amount, but if you search a computer with a terabyte of information, that is 2.5 thousand tons of paper when printing it. That is a huge challenge. And evidence might be missed, there is also a risk of missing something that is in favour of the suspect and then, in retrospect, the police and the prosecutors might be perceived as biased. This is a general challenge in securing evidence in IT environments [...] and with these large amounts of information, sometimes one must choose to only focus on and investigate a certain part of it, if not, one cannot pull it off.’ (Interview 6)

As the interviewee says, the new type of evidence that is generated in cyberspace is information instead of physical items. The amount of documentation that this information produces creates a risk of evidence being missed, espe-

cially when the investigators even at an initial stage have to focus on specific parts of the material and leave other parts without inquiry.

The interconnectedness of the above-mentioned four aspects of information difficult to discover can be seen not only in their occasional dependence on each other but also in their common denominator, which is the time aspect. Furthermore, these four aspects can affect or interact with each other in an investigation making the time span even longer. For example, in order to decrypt information, legal aid is necessary. Legal aid takes time. Decryption takes time. The encrypted information then indicates that a third country is involved and an IP number can lead to a suspect. Once again legal aid is needed, which takes more time. When the request for legal aid is answered, six months has already passed and the information concerning the IP number is deleted. Or, it could even be the case that the amount of encrypted information was so vast that the investigators only focused on one part of it, missing the evidence and the IP number from the beginning.

The overall difficulty in investigating cybercrime is therefore the time not being enough to investigate the cases to the full, as expressed by an interviewee.

4.6.5 Cooperation

The cases in our study have shown that there are multiple criminal offences within the cybercrime set-up, some occurring together more commonly than others. One of our cases (K16) involved tax offences, accounting violations, the evasion of tax inspection, forgery and the use of counterfeit documents, illicit gambling and fraud. In addition to this, some of the group members were also charged with instigation to attempted murder and attempted murder.

As we explained in the descriptive section of the police organisation, the cyber aspect is not an integrated part of the work. This is, however, not the only aspect that seems to be independent. Almost all crime areas are viewed as distinct and separate parts. To be able to investigate a horizontal crime with many different aspects, which many of the cyber-related crimes have, when the organisation is vertically formed, collaboration is naturally an important factor while also being a challenging factor.

‘Usually, the police have an organisational focus based on tunnel thinking. If we have a case of fraud, we investigate that particular incident of fraud by itself, and then similarly, if we have computer hacking, we would investigate that specific hacking, that Trojan by itself. But organised crime, that’s a matter of a large set-up, like, it starts with hacking and it ends with fraud. Because the set-ups are very lateral, they are not shaped like a tunnel, they start somewhere and

then it spreads across many different areas to generate an economic gain for the offenders in the end.’ (Interview 1&2)

Internal collaboration

‘Considering the scarce resources we have, our collaboration is good.’ (Interview 1&2)

The quote reflects the general opinion within the police: they experience functioning collaborations and there is a view of collaboration as a natural part of the work, to the extent that it is possible. This last part of the sentence needs to be highlighted: to the extent that it is possible. Just because the experience is positive does not mean that it is highly developed. As the quote says, the resources are scarce and therefore have to be administered carefully. This means that cooperation might not be an integrated part of every necessary step of the investigation but that collaboration between the different units is always present when essential.

One could say that this, too, is a question of time. For example, there are few IT forensic analysts in relation to the requests generated by the investigational units. Thus, if an investigator needs help from an IT forensic analyst, he or she knows that the waiting time might be long. Sometimes, as mentioned previously, investigations cannot wait to incorporate evidence in the preliminary investigation and the evidence is then not presented as part of the case. In other cases, it means that the investigator needs to prioritise which material is key and needs to be analysed by the IT forensic analyst. Other important evidence is thus ignored through this prioritisation. The same principles relate to contact with other investigational units. If the resources are scarce, they might not always have the time to allocate and one therefore does not always ask.

External collaboration

Collaboration with external contacts is described as sporadic and with room for improvement. We have already described the value of good collaboration between various authorities, national and international actors as well as between the private and public sector. We have also mentioned some of the bottlenecks in these procedures. Moreover, despite its importance, external cooperation is not a highly developed and integrated part of investigations. When asked about the lack of structure in external cooperation no concrete explanation was found. Some say it could be because of the lack of resources, others say it might be due to bad communication channels between the actors. A third voice says it could be based on an old practice of not using the potential of collaboration partners.

However, it is not only a question of collaboration partners. The interviewees also identified various areas of the criminal spectrum where cooperation is

important. Once again, the investigatory part is regarded as being improved by cooperation. However, crime prevention is highlighted as a subject where more effort would result in vast improvement and where the interviewees themselves think they are lacking.

4.6.6 Detection and confiscation of assets

When asking one interviewee if she thought that they confiscate the majority of the profit of crime in their cases she answered quickly ‘No, that would only be boasting if we thought that’ (interview 7). The reason for the difficulties in the detection and confiscation of assets has proven to be threefold and is mainly due to the difficulty in identifying the assets.

First of all, rapid money transfer systems are increasing, both in speed and in numbers of users. The second aspect concerns the destination of the money. As described in 4.2, a vast amount of the profit is transferred abroad. Once again, when matters become international, the process is slowed down and sometimes disrupted. Both the interviews and the case study show that when the police contacted international banks to confirm fraudulent behaviour or to inform them that certain accounts at their bank had been targets of fraud, sometimes little or no answer was received. If it is a question, then, of identifying the holder of an account, the person might not be identified, or it is a case of mules.

Thirdly, encryption hinders the identification of what assets are profits of criminal activity. For example, if a Cyber-OC group is selling narcotics over the internet and all communication between buyers and sellers is through encrypted email, little information is left for the police to track what revenue is generated from the illegal activities.

As said, these three above-mentioned aspects mostly affect the task of identifying the assets. As another interviewee said, when the profit is identified, they have fairly good authority to confiscate it. However, there is a growing problem regarding confiscation as well: digital currencies.

‘It is about applying the existing legislation and rules to new technology, we are talking about new means of payment, cryptocurrencies, where we do not have any physical money that we can actually see and tear apart and thus confiscate. Now we have a value that is written there somewhere, it is very diffuse.’ (Interview 1&2)

With the ubiquity of the use of digital currencies, a new question arises: how does one confiscate it? For now, the only answer we can give is that the Swedish Prosecution Authority is starting a project regarding this during the autumn of 2015.

4.6.7 Challenges, bottlenecks, experiences and best practices

This section focuses on the challenges and best practices of the police investigations that were not discussed in earlier sections.

Legislation

As our interviewees and cases have shown, there is a gap between legislation and reality. This means that current legislation was written and formed in a time not as technologically developed as today. Police and prosecutors are therefore encountering situations where either legislation is inadequate and ambiguous or where there is no legislation applicable. This is exemplified by one of our interviewees:

‘What we need is the opportunity to view information in a new and modern way. The legislation is mainly based on old principles of seizure, where the aim is to get hold of a specific object that exists at a particular location. To access this item you do a search, you take the object and put it somewhere and then you write a seizure protocol. But today, the key to what we do when we make seizures in IT environments is the principle of information. It is usually the information that we want to access.’ (Interview K14)

Secret data reading (hemlig dataavläsning)

Already in 2005 a Swedish Government Official Report dealt with the question of ‘secret data reading’ and its implementation. Back then the legislator rejected such an implementation (SOU 2005). However, the question is still a topic. Today, the investigatory authorities can only gain access to the communication between computers, when the information is already encrypted. ‘Secret data reading’ would enable the authorities to hack a suspect’s computer and to plant a software (a ‘spy Trojan’) that would secretly record what is happening in the computer and report it to the authority. Thus, the information is accessed before being encrypted. This method is already used in other countries, Denmark for example, and it could be very useful for Swedish law enforcement agencies.

Digital search warrant from a distance

While Cyber-OC is global, the law enforcement authorities are not. They have limitations and boundaries based on the geographical borders of the nation and the national law. This dichotomy has raised practical questions in relation to the securing of evidence and to the information gathering in an IT environment.

As we already touched upon, information accessed from a computer or mobile phone does not necessarily mean that the information is stored on that particular device. It could be a question of cloud services, emails saved in the draft folder of an email account or any other circumstance that includes the

use of a server. It is on this server that the information is stored and the information is thus the property of the company or person who owns the server.

When the investigators want to access the information, they cannot collect it directly from the cloud service, email account etc. That would be a question of computer hacking in relation to the server and the company or person owning it. Instead, they would need to contact the owner with a request. A tactic of cybercriminals is that they use servers in various countries, usually located far away from and with a different legislation than the countries they are committing their crimes in. This means that the process would include legal aid, which in itself is a problematic part of investigations, as shown before. When the legislation differs between the requesting and requested country, it might become even more complicated.

A solution to this would be a digital search warrant from a distance, where the law enforcement authority has the right to gain access to the server through the internet connection and to download the information legally. An example of this is Belgium, where all information accessible from Belgium can be legally retrieved by the investigatory authorities regardless of the country the server is located in.

Shutdown of websites

The Swedish legislation does not enable the law enforcement authorities to shut down a web site. This might not be a central part of the investigatory work, but it would be a particularly successful strategy of crime prevention e.g. in cases of file sharing or online pharmacies that sell narcotics. Denmark as an example has determined that if a person with strong connections to an illegal website is arrested, it is justification enough to shut this website down.

Human Resources

It is not enough to have the necessary equipment to carry out IT forensics, expert staff is also required. Today, the police do not have enough IT experts to meet the demand, and tasks are piled up with a long waiting time. One interviewee said that there are some prosecutors that even say that there is no point in seizing computers because they will not have the time to investigate them anyway (Interview K4). Another interviewee said that it can take up to one or two years to get IT forensic results back (Interview K14).

More and more cases have ICT evidence that needs to be retrieved, regardless of the crime types and range. Since IT forensics are understaffed and the number of errands with the need of IT forensic grows, not even all cases of serious offences are guaranteed assistance (Interview K13). In practice, this means that it is the investigators who have to deal with the vast amount of electronic information and by themselves try to find things of interest in the

material. There are of course limitations since the investigators do not have access to the equipment and software needed to enable a thorough search of the material. Hence, trying to find evidence is like looking for a needle in a haystack.

Lastly, investigations of cyber-related crimes are very time consuming, much owing to the vast amount of information generated as soon as ICT is involved but also since the evidence tends to be in the details. More personnel in general, e.g. IT experts and investigators of all sorts, are therefore needed alongside with time allocated for them to investigate.

Cyber, the sixth sense

The last aspect of practices that caused bottlenecks or challenges is a subject that we have accounted for previously and concerns the fact that cybercrime is not an integrated part of the investigatory organisation but is instead viewed as a topic by itself.

The police lack a clear rule of procedure on how to manage large amounts of electronic information, which is today the norm regardless of the crime type. Whether it is a case of rape, robbery or hacking, the investigators deal with large amounts of ICT-related information, primarily from mobile phones, which today contain everything about a person's life. Due to the lack of a clear rule of procedure there are deficiencies in the skills and abilities of the investigative staff and they have neither the time nor the capacity to handle the information. We previously described this as looking for a needle in a haystack and it can at worst lead to the situation of having the information needed to prosecute a person for the crime, but being unable to detect it.

5 Concluding remarks for Sweden

In order to get material that is comparable to the other national reports, we have chosen to structure the concluding section in line with the research questions. Thus, we create a basis for comparative study, where the basics have already been covered and where room is left for shared discussion and conclusion.

5.1 Involvement of OC in cybercrime

The majority of the cases are computer-assisted . . .

The general result of our data collection and analysis has shown that the majority of the organised groups in our study carried out computer-assisted crimes. This means that the cyber connection in our cases does not necessa-

rily consist of more than the usage of internet or computers as a tool in the criminal activity (in contrast to computer integrity crimes and computer content crimes where the cyber connection centres around it being both the fundamental link and the scene of the crime). Since computer-assisted crimes do not necessarily contain an integrated cyber aspect at every step in the *modus operandi*, and the criminals do not necessarily need any high technical knowledge, computer-assisted crimes are the easiest cybercrimes to commit. Thus, it is not particularly surprising that this category constitutes the majority of our cases. There are, however, different procedures in the usage of the internet and computers when committing computer-assisted crimes and these will be described throughout this section.

... but they can also occur in combination with other types of cybercrimes

There are, of course, exceptions and variations within this general result; there are a few groups who were involved in computer integrity crimes as well as crimes involving cryptomarkets, however, both usually in combination with computer-assisted elements.

We can also see that some computer-assisted cases were preceded by acts of computer integrity crime committed by someone outside the group. This structure, where the group's cyber-assisted crime is enabled by a computer integrity crime already carried out by someone else, is particularly apparent in the category of organised crime that develops in an ICT environment and mainly concerns cases of fraud. It is usually a question of a group of criminals buying information, such as credit card information or email addresses and passwords, over the internet or through cryptomarkets. This information is sold by someone who has obtained it through e.g. hacking, a computer integrity crime, or through skimming, a computer-assisted crime. The purchase of the information is classified as a computer-assisted act. The groups then use the information to e.g. commit fraudulent purchases online, once again a computer-assisted act. So even if the group who carried out the fraudulent behaviour are only involved in the part of the crime defined as computer-assisted, it is still possible that it is based on a computer integrity crime as well. However, the usage of the internet enabled the retrieval of the information as well as the fraudulent behaviour. The internet is thus enabling criminal groups to profit from crimes that they would not have been able to commit in their current form.

The absence of computer content crimes

Lastly, what we have not seen is any cases of computer content crimes. We can conclude that this probably depends on the nature of the crimes within this categorisation and the infrequency of them being carried out by an organised criminal group.

5.2 Using the internet to commit offline OC

As said, the majority of the cases were computer-assisted crimes. This is particularly so in the category of traditional organised crime that enters the internet. In these cases, ICT is used as a tool in order to gain advantages, usually in terms of effectiveness and profit maximisation, and is replacing former procedures. This can take several different forms but we have identified three areas of conduct in which ICT is commonly used and the underlying causes of the usage.

Firstly, it mainly replaces a more traditional form of communication. In relation to suppliers, buyers and victims, this is mostly done through websites and cryptomarkets and sometimes online communities, where one can advertise and order products. This new online contact space generates a broader audience for the crimes committed and ultimately global distribution and access. New methods of communication are also used in relation to the groups' internal communication. Online communication through encrypted email and computers, information sent through apps or cloud services is used with the purpose of avoiding detection or hindering evidence retrieval in case of a trial. It also enables group members to be globally located while working together.

The second area of conduct is in relation to money transfers. Cryptocurrencies, online banking and payment methods are used by Cyber-OC groups committing traditional organised crimes online. The purpose is to increase the anonymity of the offenders as well as to retrieve the profit as quickly as possible from a global market.

Lastly, ICT is used as a tool in relation to control. Since the two previous areas of conduct have enabled a global market, the criminal groups need to be able to control their global activity. This can be done through software and an internet connection, where exact revenues, expenditures, percentages, etc. are logged. This not only facilitates administration but also reduces the risk of being deceived by persons involved at a distance.

In sum, the new channels of communication, payment and control are making the criminal activity more effective through an increased area of operation and a reduced time input. In the end this also contributes to a maximisation of profit.

5.3 Windows of opportunity for OC groups

New windows of opportunity for the development of new business ideas

In relation to new opportunities and as stated and exemplified in the first subsection, the internet enables criminal groups to profit from crimes that they

would not have been able to commit in their contemporary form. To develop this further, the internet enables outsourcing and splitting things up within criminal set-ups. This provides criminal opportunities of cooperation between people with special expertise, criminal ideas and necessary contacts. In addition to this, the internet also connects these people and enables the collaboration in practical terms irrespective of the geographical distance. In this way, the internet connects people and groups who by themselves would not be able to commit the chain of acts necessary for the crime.

Additionally, through the use of the internet, criminal groups can utilise the differences in national legislation to their advantage and can operate from afar through the new methods of communication, payment and control.

New windows of opportunity for OC groups to identify and approach new targets

This sub-section will be divided into targets of crime who are unaware of it and those who are aware. We will start by covering the first group mentioned: targets who are unaware.

This group is strongly represented in the category of organised crime that develops in an ICT environment, and is characterised by the fact that the criminals do not want their targets to be aware of the criminal act. With traditional means, this would have been cases of robbery, cheque fraud, etc., where the criminals actively sought out their victims. By using the internet, the criminals do not need to take an active part in identifying and approaching their targets; the technology makes the victims come to the criminals. By using credit cards, computer banking, online shopping, emails, etc., the everyday person provides the information needed for them to become victims. This information is then transferred to the criminals through skimming equipment, hacked databases, Trojans, ransomware, worms and viruses. Thus, criminal groups do not need to actively and individually identify targets; the internet does it for them.

The second type of targets refers to people who are aware of the criminal activity. This type of targets is common within the category of traditional organised crime that enters the internet, and they are usually a form of customer more than a victim. This also means that the target approaches the criminal group for specific services or products; traditional examples of this are drug sales and prostitution. As we have described in this report, these types of crimes are entering the ICT environment through the use of marketing channels e.g. websites and online ads. Hence, the clientele, i. e. the targets, are located on a global market instead of a local one and the criminal activity can be accessible from afar. ICT has thus not provided a new opportunity but developed and enlarged an already existing procedure.

5.4 Structural changes in OC

Traditional OC that enters the internet

We have not seen any structural changes within the groups involved in traditional organised crime that enters the internet; they are still hierarchic and stable in their structure and they are committing the same type of crime as before, usually by the same means. The only difference is their usage of the internet as a communicative tool in relation to their targets. This nevertheless does not change the set-up of the criminal activity and should instead, as stated, be viewed as a tool for an already existing procedure and not as a new *modus operandi*.

We have, however, seen a few minor changes in direct relation to the ICT connection. Since the groups are operating on a global market, some cases have involved people in the group moving abroad for the criminal activity to proceed. Owing to the global market, the criminals have started to communicate with internet-based solutions such as Skype, emails or apps. Since ICT knowledge is sometimes needed to a limited extent, some new contacts have been made in order to construct or handle the ICT tool. However, does this induce structural changes? No.

OC that develops in an ICT environment

Regarding organised crime that develops in an ICT environment, some structural deviations are visible in relation to traditional OC. Since the internet is enabling contacts and new opportunities for splitting things up and outsourcing, there is a visible change in the initiation of the crime and group. When traditional OC groups are initiating a criminal activity, the crime emanates from the group. In these cases, the group often follows the idea, i. e. a criminal set-up is thought of and the group is formed around the idea and based on the skills needed. This affects the structure of the groups and they become more changeable than stable. Every set-up can therefore involve new actors within the group. Since the idea is the fundamental link and the actors are variable, the hierarchic structure is not as cone-shaped and the positions of the people involved are more 'floating'. As a consequence of the changeable structure, outsourcing and collaboration between groups and actors can occur more frequently. This affects the traditional division of labour, where the group usually controls and performs the entire criminal activity. In organised crime that develops in an ICT environment, separate groups can interchangeably own different parts of the criminal chain, making a profit out of their individual part. The *modus operandi* is thus also different. In addition to this, one can see that with the increasing use of the internet, technology in itself becomes an actor that is as important as the criminals themselves.

In sum, since the category of organised crime that develops in an ICT environment is based on usage of the internet, changes have occurred within the group's initiation process, structure, division of labour and modus operandi.

5.5 The organisation of cybercrime

There are two types of organisational forms visible, which can be viewed as two poles. In between that span, a variety of versions can be found.

The first pole is one of a closed organisation composed of specific never-changing actors. The activity of the group is all controlled and handled within this well-defined circle of people and the organisational form is constant over a long period of time and different activity variations.

The second pole consists of single individuals that on their own initiative come into contact with other single individuals and create a long branchy chain of individual encounters. One could argue that this is not the definition of organised groups but one important aspect needs to be taken into consideration before one gives way to that opinion. Would the individuals who contact other individuals have been able to implement their criminal activity if not for the contacts made and the previous contacts of that contact? The answer is no. The act of one single person is dependent on the contacts and the entire chain is thus performing the role of an organisational collaboration where every actor contributes with a specific task.

These two poles create a span between which multiple variations and combinations can be found. The aspects that the organisations tend to be closer to or further away from are: collective or individual, stable or unstable, autonomous or collaborative and common goal or individually driven.

5.6 Recommendations

We have listed various bottlenecks throughout the previous sections and it is now time for a comprehensive approach in relation to improvement. The recommendations will follow the structure of crime prevention and investigative work while differentiating between procedures and legislation.

5.6.1 Crime prevention

As we have mentioned, the criminal usage of the internet creates an inverse relationship where potential victims provide information that the criminals can easily use to target the victims. It is thus important to actively and in-

creasingly spread information to the general public regarding various risks of internet usage. This is to enhance the public awareness of how to act in relation to internet banking, passwords, emails from unknown addresses, 'to-good-to-be-true' offers, etc.

It is also important to spread information in relation to more traditional crimes such as online pharmacies and counterfeit goods. The goal is twofold and the aim is firstly for the general public to understand the difference between original products and forged products in relation to quality, legality and health risks. Secondly, it will also reduce the demand for such products, which makes the activity less attractive for criminals.

In order for the dissemination of information to be successful, all actors in society that are affected by the criminal activity need to participate and spread their share. This includes law enforcement authorities, authorities with a connection to the specific area of the criminal activity, private actors involved with the internet and ICT, banks, etc.

5.6.2 Investigative work

Education

As stated when discussing bottlenecks, the cyber aspect is not an integrated part of the police organisation. This means that the general level of ICT knowledge in relation to investigatory work amongst the investigators is rather low. This affects the investigation at an initial stage. For example, information could be erased, leads in the cyber world may not be thought of, and vast amounts of information may not be investigated in an effective way. An educational initiative is thus recommended, where the police organisation would educate all investigators, regardless of their specialisation, in the basic investigatory work of cyber-related practices.

We would also recommend that the police provide cyber-related training directed to their officers who meet the victims and work with formulating the police report. By asking for the right information already at the first contact, the right type of information is received, which can demonstrate that the case has investigatory leads and evidence and should not be closed. In addition to this, the investigator can, when given a comprehensive picture of the case, initiate the work faster and therefore also have a greater chance of solving it.

In the long run this will create increased confidence in the police from the general public as well as an incentive for reporting cyber-related crimes.

Legal aid

In order to improve the procedure of legal aid, particularly with the aim of shortening the time span between requests and answers, we recommend an international review of the possibility of decentralising the process of handling and establishing direct channels of communication between national authorities.

A common position

Owing to the difference between the global character of Cyber-OC and the national character of legislation, we recommend Sweden as well as every nation at least within Europe to continuously discuss and work towards a common position of law enforcement legislation.

6 References

- Brotsförebyggande rådet (Brå), 1981, Brotsutveckling, Lägesrapport 1981.
- Brotsförebyggande rådet (Brå), 2000, IT-relaterad brottslighet, Stockholm, Tierps Tryckeri AB
- Brotsförebyggande rådet (Brå), 2008, IT-relaterade brott och incidenter Ett hot mot samhällsviktiga verksamheter?, Stockholm, Brotsförebyggande rådet, Information och förlag
- Brotsförebyggande rådet (Brå), 2012a, Användningen av brottskoder. En kvalitetsstudie inom kriminalstatistiken, https://www.bra.se/download/18.1ff479c3135e8540b29800021266/1371914739137/2012_An-v_ndningen^v_brottskoder.pdf (2015-11-02)
- Brotsförebyggande rådet (Brå), 2012b, Kodning av brott, anvisningar och regler, https://www.bra.se/download/18.22a7170813a0d141d21800050764/1371914741414/Brottskodningslistan-2012+v11_3.pdf (2015-11-02)
- Brotsförebyggande rådet (Brå), 2012c, Brotsutvecklingen i Sverige 2008-2011, Elanders Sverige AB
- Brotsförebyggande rådet (Brå), 2015a, Polisanmäla hot och kränkningar mot enskilda personer via internet, Lenanders Grafiska AB
- Brotsförebyggande rådet (Brå), 2015b, Kriminalstatistik 2014, Lenanders Grafiska AB
- Castells, Manuel, 1999, The rise of the network society, Blackwell publisher
- Försvarets radioanstalt (FRA), 2011, FRA årsrapport 2010, <http://fra.se/download/18.24cbfd712f970f10a78000127/0386-arsrapport-2010.pdf> (2015-11-02)
- Försvarets radioanstalt (FRA), 2013, FRA årsrapport 2012, http://fra.se/download/18.17ed2a0913b91344b7b8000163/FRA_Arsrapport_2012.pdf (2015-11-02)

- Försvarets radioanstalt (FRA), 2014, FRA årsrapport 2013, http://fra.se/download/18.24e50f31145229e353f80001/FRA_Arsrapport_2013_webb.pdf (2015-11-02)
- Goldberg, Daniel; Larsson, Linus, 2011, Svenska hackare – En berättelse från nätets skuggsida, Nordstedts
- Kronqvist, Stefan, 2013, Brott och digitala bevis, En handledning, Vällingby, Elanders Sverige AB
- Myndigheten för samhällsskydd och beredskap (MSB), 2015, Informationssäkerhet – trender 2015, Danagård LiTHO
- Polismyndigheten, 2014, Polisen, arbetsordning för Polismyndigheten, http://polissamordningen.se/filer/Arbetsmaterial°ch_beslut/Fattade%20beslut/Arbetsordning/Arbetsordning%2020141114%20slutlig.pdf (2015-11-02)
- Polismyndigheten, 2015a, Faktablad Den nya Polismyndigheten, <https://polisen.se/PageFiles/563212/NYA%20POLISEN%20Faktablad150304.pdf> (2015-11-02)
- Polismyndigheten, 2015b, Polismyndighetens it-strategi för 2015-2017, https://polisen.se/PageFiles/556779/Polismyndighetens_It-strategi_2015-2017.pdf (2015-11-02)
- Post- och telestyrelsen (PTS), 2013, Konsumenters förhållande till Internetsäkerhet, <http://www.pts.se/upload/Rapporter/Internet/2013/rapport-konsumentundersokning-om-internetsakerhet-131002.pdf> (2015-11-02)
- Regeringskansliet, 2011, It i människans tjänst – en digital agenda för Sverige, Stockholm, åtta.45
- Rikskriminalpolisen (RKP), 2005, Narkotikaspaning på Internet; slutrapport Projekt Nicks, https://www.polisen.se/Global/www%20och%20Intrapolis/Rapporter-utredningar/01%20Polisen%20nationellt/Narkotika/Narkspan_pa_internet.2005.pdf (2015-11-02)
- Rikspolisstyrelsen (RPS), 2014, Inspektion av polismyndigheternas förmåga att handlägga IT-brott, Tillsynsrapport, https://polisen.se/Global/www%20och%20Intrapolis/Rapporter-utredningar/01%20Polisen%20nationellt/Ovriga%20rapporter-utredningar/Inspektioner-tillsyns%20rapporter/2014/Tillsynsrapport_14_2_it%20brott.pdf (2015-11-02)
- SOU, 1992, Information och den nya Informations Teknologin – straff- och processrättsliga frågor mm., SOU 1992:110
- SOU, 2005, Tillgång till elektronisk kommunikation i brottsutredningar m.m. <http://data.riksdagen.se/fil/5DA6159A-159B-4B2D-91A2-6F425DF54DBC> (2015-11-02)
- SOU, 2015, Informations- och cybersäkerhet i Sverige; Strategi och åtgärder för säker information i staten, Stockholm Elanders Sverige AB
- Statistiska Centralbyrån (SCB), 2011, Anmällda brott, http://www.scb.se/Statistik/RV/RV0102/_dokument/RV0102_BS_2011.pdf (2015-11-02)

Statistiska Centralbyrån (SCB), 2014, Privatpersoners användning av datorer och internet 2013, http://www.scb.se/Statistik/_Publikationer/LE0108_2013A01_BR_IT01BR1401.pdf (2015-11-02)

Säkerhetspolisen, 2012, Säkerhetspolisen 2011, Danagård LiTHO

Säkerhetspolisen, 2014, Säkerhetspolisen 2013, Edita

Säkerhetspolisen, 2015, Säkerhetspolisens Årsbok 2014, Edita

IV. Cyber-OC in Germany

G. Bulanova-Hristova, K. Kasper

The following case study presents an approach for describing Cyber-OC based on the parameters that have become evident in Germany. The emergence of Cyber-OC is attributed, amongst other things, to the rapid development and global networking of information and communication technology (ICT) that has been witnessed in recent years. This phenomenon is a challenge to domestic security that arises from the merging of two particularly dangerous forms of crime – cybercrime and organised crime – and thus presents a major potential threat. What exactly is behind this ‘criminal merger’ and how it manifests itself in Germany is one of the central questions of this case study.

Since it deals with a controversial criminal phenomenon, the essence of which has barely been researched yet, and for which a firm definition cannot be expected in the near future, investigating this phenomenon represents a challenge in terms of methodology and definition. In order to be able to tackle this complex task, first of all an internal working definition for the project was defined that forms the basis of the empirical analyses in all three participating countries.

This way the cumulative nature of the Cyber-OC phenomenon – as the interface between two areas of crime – will be reflected from two perspectives: on the one hand it will ensure that the analysis is based on an internationally agreed understanding of organised crime, and on the other, it will draw on a widely cited typology of cybercrime, which also reflects the subdivision of cybercrime into a narrow and a broad sense undertaken in Germany.¹⁰⁸

In summary and based on these principles, Cyber-OC comprises crimes that are committed collaboratively and methodically by criminal groups and that are aimed at the internet and other forms of ICT or are committed using these. Accordingly, this understanding of Cyber-OC comprises cybercrime by ‘traditional’ organised groups as well as cybercrime committed in an organised manner.

The following section contains a short overview of the national context concerning the law enforcement system as well as some statistics on cybercrime and organised crime. Afterwards the methods used in the German case study are explained (2 Methodology). Subsequently, the results of the inquiries into

¹⁰⁸ Based on the German Police Crime Statistics (PKS) and the Federal Situation Report on Cybercrime, this project distinguishes between cybercrime in a narrow sense and cybercrime in a broad sense. According to the Federal Situation Report on Cybercrime, cybercrime encompasses actions where the internet, data networks, information technology systems or their data are the target of criminal conduct (cybercrime in a narrow sense), as well as crimes where this information technology is used as a means (cybercrime in a broad sense) (BKA 2013b: 5).

different police units for relevant cases as well as some analytical implications of their content are discussed (3 General description of the reported criminal investigations). After that, the results of the file analysis regarding suspects, groups' structure, modi operandi, damage, and investigation process are described (4 Empirical findings). The conclusion contains the answers to the research questions from the perspective of the German case study findings (5 Concluding remarks for Germany).

1 Context information

The Federal Republic of Germany is composed of 16 federal states, which are in charge of police matters. The State Criminal Police Offices (Landeskriminalämter) principally mirror the central contact point for every respective state. Moreover, they are subordinate to the Ministry of the Interior of the corresponding state. Owing to the federal system in Germany, the legal basis for preventive action within the federal states differs, whereas the legal basis for repressive actions, including the code of criminal procedure, is mandatory for every state and the public prosecutor's office.

With reference to Cyber-OC, the particular state police forces basically conduct investigations, for instance in the fields of organised crime and cybercrime, on their own, for they each have their own units for investigating in these fields (Groß 2012: 1; Groß 2008: 1–5). Overall, the state police units are primarily responsible for the criminal prosecution and the fight against cybercrime and organised crime. On a federal level the BKA is responsible among other things for the collection and analysis of information (central agency) and holds an original law enforcement jurisdiction to investigate, among other things, international organised crime (§ 4 (1) 1 and 3 BKA law) as well as most cases of cybercrime in a narrow sense if it targets 'a) the internal and external security of the Federal Republic of Germany or b) sensitive parts of facilities of vital importance whose failure or destruction could entail considerable threats to human life or health or which are indispensable for the functioning of the community' (§ 4 (1) 5 BKA law).¹⁰⁹ Furthermore, the BKA not only has original law enforcement jurisdiction, but also secondary jurisdictions which relate to cases at the request of a competent state authority, by order of the Federal Minister of the Interior, and at the request of, or on instructions from the Federal Prosecutor General (§ 4 (2) BKA law).

The BKA has to fulfil numerous tasks in the fight against crime, such as operating as central agency, international cooperation, criminal prosecution, ward-

¹⁰⁹ Cf. BMI 2016.

ing off dangers arising from international terrorism, protection of members of the constitutional bodies, and witness protection (BKA 2016). The division ‘Serious and Organised Crime’ of the BKA, which investigates in the field of cybercrime among others, not only investigates these cases but also analyses significant information on crimes and perpetrators. One result is the creation of yearly National Situation Reports on severe fields of crime, such as cybercrime and organised crime.

The growing digitalisation of the world affects multifarious areas of life and increases the overall interconnectedness. Ergo, the seemingly infinite possibilities of the internet create new opportunities for criminals to target and pick their victims (BKA 2013b: 11). These opportunities can be subsumed under the following areas of crime: e.g. computer fraud, data tampering, computer sabotage, forgery of data intended to provide proof and spying/interception of data (BKA 2014: 6). According to the approach of the Police Crime Statistics (PKS) and the National Situation Report on Cybercrime, a distinction between cybercrime in a narrow sense and cybercrime in a broad sense is necessary. With reference to the National Situation Report on Cybercrime, cybercrime includes ‘[...] crimes aimed at the Internet, data networks, information technology systems or their data [which refers to cybercrime in a narrow sense], [as well as crimes] that are committed using this information technology [which refers to cybercrime in a broad sense]’ (BKA 2013b: 5).

As to the understanding of organised crime, for Germany there is no legal definition in place. However, the police use the following working definition adopted in May 1990 by the joint Judiciary/Police Working Group: ‘Organised crime is the planned commission of criminal offences determined by the pursuit of profit and power which, individually or as a whole, are of considerable importance, if more than two persons, each with his/her own assigned tasks, collaborate for a prolonged or indefinite period of time a) by using commercial or business-like structures, b) by using force or other means of intimidation, or c) by exerting influence on politics, the media, public administration, judicial authorities or the business sector’ (BKA 2014a: 6).

The Police Crime Statistics reveal that crimes involving the internet as an instrument of crime (cybercrime in a broad sense), have increased from about 167,000 in 2008 to about 257,000 in 2013. At the same time the clear-up rate dropped from nearly 80 per cent to about 62 per cent (BKA 2014b: 3). Similarly the number of offences in the field of cybercrime in a narrow sense also increased during this period, namely from 38,000 in 2008 to 64,000 in 2013. The clear-up rate being already on a relatively low level in 2008 at 38 per

cent even dropped to 25 per cent in 2013 (BKA 2014b: 3).¹¹⁰ Thus, in both areas of cybercrime the total number of offences has risen significantly, which clearly shows the danger of cybercrime.

The National Situation Report on Cybercrime from 2014 states that the damage and threat potential of cybercrime increased further. Moreover, the structure and the *modi operandi* of perpetrators have significantly changed as they do not merely commit crimes, but also enable crime as they sell the necessary equipment such as malware or whole infrastructures on the underground economy. Accordingly, this equipment can be used by perpetrators without specific IT skills, which simultaneously broadens the range of perpetrators (BKA 2014c: 14). Correspondingly, organised perpetrator structures, like in ‘traditional OC groups’, are gaining more and more importance (BKA 2014c: 14).

With reference to the National Situation Report on Organised Crime in 2014, it can be concluded that the total number of investigations against OC groups is almost the same compared to the previous years (BKA 2014a: 29). However, the threat potential arising from organised crime remains fairly high owing to its entering into new fields of crime, which is stimulated by the increasing importance and impact of the internet (BKA 2014a: 29). The organised crime perpetrators remain flexible and mobile as they act across crime fields (BKA 2014a: 29). The trans- and internationality of OC remain a characteristic of OC groups because of their origin, cross-border actions and the broad range of nationalities (BKA 2014a: 29). More significantly, the OC National Situation Report claims that ‘the number of cybercrime-related OC investigations doubled from 6 in 2013 to 12 in 2014 (BKA 2014d: 25). The ongoing trend of cybercrime establishing itself in OC can also be seen in the financial damage these groups caused (41.1 million euros compared to 15.1 million euros in 2013) (BKA 2014d: 25). Overall, the threats emerging from the scope and manifestations of cybercrime are likely to increase in their intensity and quantity (BKA 2014c: 14).

2 Methodology

The working definition forms the basis for identifying criminal investigations that represent the Cyber-OC phenomenon in the countries participating in the project (totality). Here it was necessary to create an overview of all the crim-

¹¹⁰ For Police Crime Statistics from 2002 – 2013: cf. http://www.bka.de/nn_257310/EN-/Publications/PoliceCrimeStatistics/2002Bis2013/pcs2002Bis2013__node.html?__nnn=true

inal investigations within the totality in order to select approx. 10 to 15 investigations (sample) to be subsequently analysed in depth for the project.

From a theoretical point of view, the totality encompasses all elements about which statements could be made (Schnell et al. 2005: 271) and would – in this case – include all Cyber-OC criminal investigations in Germany. Since a comprehensive study of this kind without any gaps can only be achieved in the rarest of cases and depends on several factors – such as the explicitness of the inquiry and completeness of the responses – the overview of German Cyber-OC investigations drawn up here represents the so-called ‘sampling population’ of the case study that covers all the cases that can possibly be considered for the sample.

A dual approach similar to that used to compose the working definition was taken for the compilation of the selection totality, which, on the one hand, focused on criminal groups that had committed crimes against the internet or by using the internet as a means and, on the other, focused on cybercrimes that had been committed by several suspects collaboratively and methodically.

To collect cases, targeted inquiries were made to federal and state authorities asking for information on ‘Cyber-OC criminal investigations’, the aim of which was to ensure that all the Cyber-OC criminal investigative proceedings carried out in Germany within a certain time frame were documented for the project:

- **First inquiry – focus on criminal groups:** organised crime investigations related to cybercrime conducted by the Federal Criminal Police Office (BKA), the State Criminal Police Offices (LKA), the Federal Police (Bundespolizei) and the German Customs Investigation Office.
- **Second inquiry – focus on cybercrime:** cybercrime investigations with several perpetrators conducted by the Federal Criminal Police Office (BKA), the State Criminal Police Offices (LKA) and the Federal Police (Bundespolizei).

2.1 First inquiry – focus on criminal groups

The annual situation reports on organised crime serve as central sources of information about the criminal groups and their activities in Germany. Accordingly, the criminal investigations documented in the situation reports were examined to see to what extent they correspond to the working definition.

A first approach was to identify only the organised crime investigations in which the main activity of the criminal group was determined to be ‘cybercrime’. In so doing the aim was to make sure that there was a link to cybercrime. The examination of this data pool revealed that between 2010¹¹¹ and 2013 only about 20 organised crime groups were documented with this main field of activity.¹¹² However, it is safe to assume that investigations in which ICT plays an important role are not necessarily documented as cybercrime, but are recorded with other fields of activity such as, for instance, environmental crime, illegal drugs trafficking/smuggling or commercial crime. That would be true for criminal investigations involving more than one area of crime, for example, in which another offence, not cybercrime, was ascertained to be the main field of activity of the group. In light of this, responses were not just required about investigations into cybercrime, but also investigations into other main activities where cybercrime still accounted for part of the activities of the criminal group. As a result, closed police investigation files (i.e. handed over to the public prosecutor’s office) from 2009 to 2013 with at least three suspects were requested. All the investigations that are listed in the National Situation Report on Organised Crime focus by definition on organised crime groups. In order to also include cybercrime committed in an organised manner, a second inquiry was carried out.

2.2 Second inquiry – focus on cybercrime

While the National Situation Report on Organised Crime is drawn up on the basis of relevant and comprehensive responses from the German federal states and from other federal authorities, the National Situation Report on Cybercrime is largely based on statistical data from the Police Crime Statistics, which provide relatively little information about further categories – such as modus operandi, the threat potential or the complexity of a crime.

Hence, it appeared that a selection of cybercrime cases from the cases listed in the PKS would do little to help achieve the objectives, which is why it was necessary to undertake the more demanding task of conducting an inquiry within the cybercrime units at the federal and local level.

¹¹¹ For technical reasons it was not possible to consider criminal investigations from 2009.

¹¹² Organised Crime Situation Reports of the BKA, http://www.bka.de/nn_195184-/EN/Publications/AnnualReportsAndSituationAssessments/OrganisedCrime-/organisedCrime__no-de.html?__nnn=true.

Based on the responses to both inquiries, an overview of all the criminal investigations conducted in Germany between 2009 and 2013 that corresponded to the working definition of Cyber-OC was drawn up (sampling population).

2.3 Sampling

In order to make Cyber-OC more tangible, the next step was to compare the descriptions of the cases of all the criminal investigations identified as a result of the inquiries with the project-specific definition of Cyber-OC, and in so doing examine the project relevance of the investigations. In the course of this evaluation of the contents of the cases, all the investigations were divided into four groups, depending on the role played by information and communication technology (ICT) in the commission of the crime: very relevant (A), largely relevant (B), partially relevant (C) and not relevant (D). The investigations with priorities A – C were included in the case selection pool.

Since a case study is not a comprehensive inquiry but a qualitative analysis of an exploratory nature, the evaluation of only approx. 10 to 15 Cyber-OC investigations was planned. The question as to which investigations would be analysed in depth was answered with a non-probability sampling procedure applied to the selection totality. The short descriptions of the reported cases built the basis for the purposive sample. In this procedure a selection based on the following content criteria was made:

- different and technically complex kinds of *modi operandi*;
- extreme values of various items (e.g. number of suspects and victims, damage, criminal earnings, cross-regional or international commission of crime);
- various crime fields;
- various kinds of *modi operandi* within a crime field;
- even distribution of investigations between cybercrime in a narrow and in a broad sense.

This purposive sample was preferred to a random sample as the selection method, because otherwise the diversity of crime fields and criminal approaches could not have been guaranteed. In an extreme case, all the selected cases in a random sample might cover only cybercrime in a narrow sense, or – even ‘worse’ – solely cases of phishing.

In addition to the described inquiries and the subsequent file analysis of criminal cases, the German case study benefited from a constant exchange with police practitioners. Moreover, further experts' feedback was gathered during interviews as well as during various workshops. This feedback was considered during the whole case study and has been integrated in the German report. Thus the results of this case study represent first empirical insights gathered on an explorative basis that cannot be used for generalisations.

3 General description of the reported criminal investigations

In both inquiries, criminal investigations from a broad range of crime fields were identified. While roughly a quarter of the cases focus on cybercrime in a narrow sense, more than three quarters can be subsumed under cybercrime in a broad sense. This shows that ICT is broadly used in different crime fields.

As described, following the two inquiries, all the responses were reviewed against the project-internal working definition of Cyber-OC and were divided into four groups according to relevance, with only cases with a relevance from A to C being considered as Cyber-OC cases.

Overall, this method allowed $N = 128$ investigations to be categorised as project-relevant. They form the so-called sampling population of the German case study, from which a sample of 18 investigations was chosen for the subsequent file analysis.

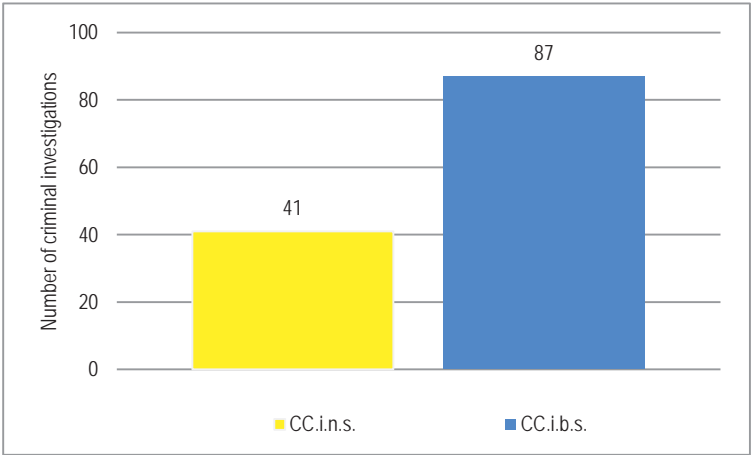
The result of this substantive review represents an overview of the criminal investigations in Germany that correspond to the project-specific understanding of Cyber-OC. Thus, an empirical study of the Cyber-OC phenomenon according to the project definition was carried out for the first time for Germany, which ought to make an important contribution to the current level of knowledge, both from the scientific perspective and the perspective of practical police work.

The following sections describe certain aspects of the cases from the sampling population, e.g. crime fields, number of suspects and damage. It has to be underlined that in contrast to the extensive file analysis (see section 5, Empirical findings of the file analysis) the following analytical implications refer to all cases within the sampling population ($N=128$) and are solely based on their short descriptions delivered by the respective police units.

3.1 Activity fields

When examining the division of offences in the criminal investigations from the selection totality into cybercrime in a narrow and a broad sense, it is striking that the internet was used in more than two thirds of the investigations as an instrument for committing the crime. Nevertheless ICT was itself the target of the criminal groups in one investigation out of three (see figure 8).

Figure 8: Division of criminal investigations into cybercrime in a narrow/broad sense (N = 128)¹¹³



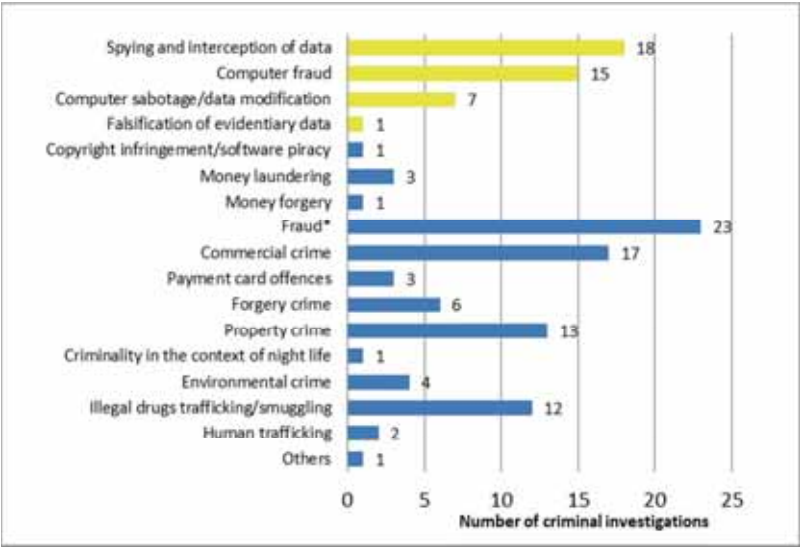
Source: IZ 34

The ‘top five’ crime fields into which most of the criminal investigations were conducted (see figure 9) were fraud (23 investigations; 18 per cent), followed by spying and interception of data (18 investigations; 14 per cent), commercial crime (17 investigations; 13 per cent), computer fraud (15 investigations; 12 per cent) and crime against property (13 investigations; 10 per cent). Based on this overview of the situation regarding investigations into the Cyber-OC phenomenon in Germany, it becomes clear that the investigations since 2009 were conducted into several people involved in the commission of the crime, both in traditional fields of crime (such as fraud, commercial crime and crime against property), but for which ICT was used as an

¹¹³ Since the categorisation of the investigations in the responses was not always clear, if an investigation covered several areas of crime, the area that was deemed the most important for the commission of the crime was chosen as the main area of crime.

instrument of crime, and in more technically complex fields – such as spying and interception of data, or computer fraud.

Figure 9: Distribution of criminal investigations to different crime areas (N = 128)



Source: IZ 34¹¹⁴

3.2 Suspects and damage

Information on the number of all identified suspects per group was provided in 84¹¹⁵ out of the total 128 criminal investigations. Of the 1,106 identified suspects, 602 committed cybercrime in a narrow sense and 504 cybercrime in a broad sense.

The 84 criminal investigations in which information on the number of all identified suspects per group was provided reveal an average group size of

¹¹⁴ *General fraud, fraud by means of illegally obtained payment card data, fraud by means of illegally obtained debit cards / credit cards. Yellow = Cybercrime in a narrow sense; Blue = Cybercrime in a broad sense. Multiple mentions possible due to dual approach of inquiry or to collective investigations.

¹¹⁵ 27 of these were criminal investigations into cybercrime in a narrow sense and 57 in a broad sense.

around 13 identified suspects (ranging between 3 and 229 identified suspects per group). It is striking that the criminal groups that committed cybercrimes in a narrow sense were significantly larger on average (approx. 22 identified suspects on average; between 3 and 229 identified suspects per group), than the groups that were involved in cybercrime in a broad sense (approx. 9 identified suspects on average; between 3 and 82 identified suspects per group). The average of approx. 22 suspects is primarily due to the perpetrator numbers in two large groups. In particular the large number of suspects in the lower levels of the hierarchy (e.g. money and parcel mules) is a key factor in the above-average number of all identified suspects per group. In large groups such as these, it is probably safe to assume that not every identified suspect has specialist IT skills or knowledge. On the contrary, the descriptions of the cases make it clear that only few of them had special IT expertise.

In order to gain a general idea of the threat potential of the Cyber-OC groups included in the sampling population, it is worthwhile examining the damage caused as well as the groups' sizes. Similarly to the examination of group sizes, it was only possible to consider the monetary damage in the investigations where information to this effect was provided in the short descriptions sent with the inquiry responses. Accordingly, the following figures indicate the amount of damage for a partial quantity of the criminal investigations and do not reflect the actual damage incurred in the area of Cyber-OC (documented here for Cyber-OC groups from the sampling population).

Out of the 128 criminal investigations, concrete information was provided in 21 cases on the damage caused by the group through fraud, fraudulent failure to supply goods as agreed / obtaining goods by fraud, unlawful online transfers from and to private bank accounts, fraudulent account opening and phishing activities, software piracy, etc. This damage amounts to almost 50 million euros overall for the criminal investigations conducted between 2009 and 2013. A third of this sum (16.62 million euros) came from seven investigations into cybercrime in a narrow sense and two thirds (33.21 million euros) came from 14 investigations into cybercrime in a broad sense.

The highest damage, at 12.2 million euros overall, was caused in the area of fraud. In two investigations each in the areas of 'economic crime' and spying/interception of data, damage of over 5 million euros caused by phishing, fraudulent failure to supply goods as agreed, fraudulent notification by telephone of prize winnings and fraud as part of the feigning of real business operations was ascertained. In another investigation in each of the two above-named areas of crime, damage of between 2.3 and 3 million euros was investigated. Hence, in the above-mentioned subset of 21 investigations, the crime fields of fraud, spying and interception of data, and economic crime represent the areas in which the Cyber-OC groups were able to cause the most damage.

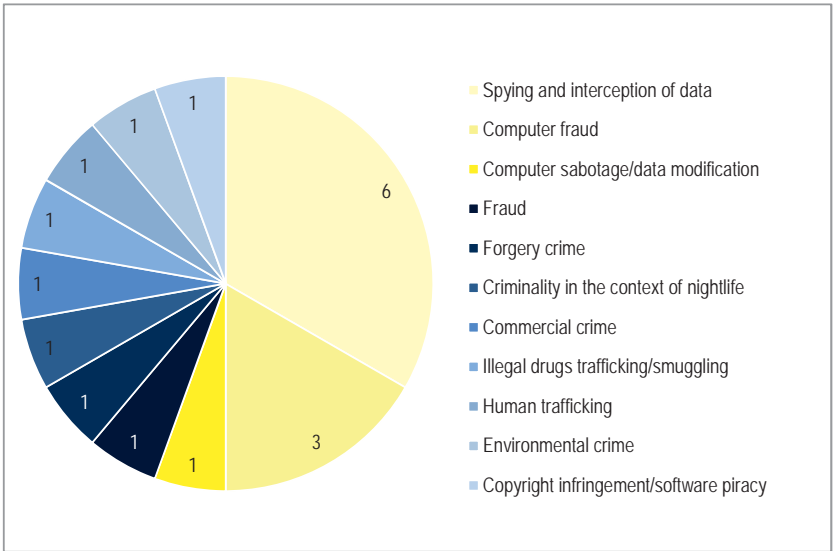
Despite the rather low figures of financial damage and considering the little information provided, it still can be assumed that Cyber-OC causes a much higher monetary damage. In addition, the non-material damage – for example to users’ trust in the integrity of computer systems, their feeling of security online, or even their own health when purchasing counterfeit medicinal products online – is likely to be much more serious. This question is going to be discussed in more detail in section 4 ‘Empirical findings’.

4 Empirical findings

4.1 Overview of the sample

A sample of 18 out of 128 cases was chosen for a detailed file analysis. They involve many different crime fields and represent a balance between cyber-crime in a narrow and a broad sense (see figure 10).

Figure 10: Distribution of criminal investigations according to area of crime (N = 18)



Source: IZ 34

4.2 Group categorisation

The examination of Cyber-OC groups within the sample allows a typology that is based on the correlation of two qualitative characteristics and thus facilitates the systematic analysis of group structures beyond the merely differentiation in terms of crime fields.¹¹⁶ As a result, four group categories were identified. The Cyber-OC groups within each category are characterised by equal characteristic values.

The characteristics ‘reason for group formation’ and ‘place of group formation’ form the basis for differentiation and are divided into two attributes each. Thereby, the characteristic ‘place of group formation’ is operationalised through the attribute ‘offline’ (the group formed in real life) and ‘online’ (the group formed on the internet). The characteristic ‘reason for group formation’ is subdivided into the attributes ‘committing of other crimes (not cybercrime)’ and ‘committing of cybercrime’. Accordingly, with respect to their formation Cyber-OC groups can be allocated to four categories, as the following chart illustrates.

Figure 11: Matrix of group categories in Cyber-OC

		Reason for group formation	
		Committing of other crimes (not cybercrime)	Committing of cybercrime
Place of group formation	Offline	Offline groups entering cybercrime (Category 1)	Offlineborn groups (Category 2)
	Online	Online groups entering cybercrime (Category 4)	Cyberborn groups (Category 3)

Source: IZ 34

¹¹⁶ As illustrated in the literature review (see appendix) there exist different typologies of cyber-crime groups based on similar characteristics. However, for the categorisation elaborated in this case study a specific combination of them has been applied.

Category 1 – Offline groups entering cybercrime (cyber-entering groups): The ideal type group that can be assigned to category 1 is characterised by the fact that its members joined forces in real life engaging jointly in criminal activities (not cybercrime). During the course of their cooperation they discover cybercrime as a further profitable source of income, thus complementing their activities with activities located in this crime field. This means that cybercrime is one of several crime fields the group is engaging in and can be seen as ‘extra income’.

Category 2 – Offlineborn groups: The ideal type group in category 2 is composed of members who know each other from real life and engage in order to commit cybercrime. Although they do not share a common criminal history, which distinguishes them from members of Cyber-OC groups in category 1, friendship or acquaintance because of socio-cultural common ground existed before group formation. Nevertheless, individual members may have a criminal background. Cybercrime is considered to be the central activity field of the group.

Category 3 – Cyberborn groups: The ideal type group in category 3 consists of members who met in an online environment e.g. a chat room, social network or forum and joined forces in order to commit cybercrime. Similar to category 2, these members have never engaged in criminal activities in this specific group constellation before. Cybercrime, too, is the central activity field of the group.

Category 4 – Online groups entering cybercrime: The ideal type group within category 4 is characterised by members joining forces in an online environment in order to commit crimes (not cybercrime). As an example one could cite multiple suspects who met in a forum and decided to sell narcotics in real life without drawing upon ICT. During the course of their cooperation they discover cybercrime as a further profitable source of income, which adds to their criminal portfolio. Similar to category 1, cybercrime comprises one of several activity fields of the group.

Whereas the following analysis identified Cyber-OC groups that were allocated to categories 1 to 3, there was no group that could have been assigned to category 4. Nevertheless the existence of such groups in the field of Cyber-OC is certainly possible. In the realm of the politically motivated crime, such groups are, for example, a fact.

4.3 Determination of the group membership

In the course of the empirical analysis, besides the possibility of a qualitative typology of Cyber-OC groups, the question of determining the group membership was raised. As a result of the suspects' specific roles, such as, for instance, the money mules,¹¹⁷ the clear determination of group membership turned out to be difficult. In order to answer the question as to who belongs to which group, a differentiated approach to the identified suspects was conducted.

Here the main suspects, amongst them externally controlling backers and knowingly involved accomplices, were appointed to the category 'core group'. Other persons involved, including unknowing, and sometimes even victimised 'supporters' were appointed to the category 'group periphery'. The category 'all identified suspects'¹¹⁸ contains both core group members and the group periphery members. In several investigations members of the core group used the support of additional services from e.g. programmers, web designers as well as hackers and forgers of identity papers (Crime-as-a-Service). Because of their solely selective support, these 'experts' were not taken into consideration when counting 'all identified suspects'. Their activity was nevertheless considered in regards to content in the analysis of the cases.

A clear allocation of groups was also not a straightforward task as the commonly used money mules and parcel mules in cybercrime were difficult to assign. Without their (unconscious or conscious) support, the crimes could not be fully committed, so they were allocated to the Cyber-OC group, however, they did not belong to the 'core', but rather the 'periphery'.

Summing up, the Cyber-OC groups consist of a 'core' and a 'periphery'. The support by accomplices from the periphery was often crucial for a 'successful' accomplishment of the crime.

¹¹⁷ Money mules are generally bank account holders who receive illegally gained money to their bank accounts and subsequently transfer (parts) of the money to other suspects. The money mules may be consciously or unconsciously involved in the crimes.

¹¹⁸ Not to be understood in the juridical way, but rather according to the Police Crime Statistics: 'a suspect is everyone who, according to the result of the investigation by the police, is suspicious due to sufficient indications of having committed a crime illegally. Included are accomplices, instigators and supporters' (Bundeskriminalamt 2014).

4.4 Summary of the analysed investigations

In the following, the analysed cases are shortly summarised, each criminal investigation having a separate project-specific case number. This allows for better comprehension and shows the diversity of crime fields as well as the diversity in *modi operandi*. The subdivision into cybercrime in a narrow sense (CC.i.n.s.) and cybercrime in a broad sense (CC.i.b.s.) does not mean that the respective Cyber-OC group was only active in *one* of the two cybercrime areas as the classification was rather based on the main focus of the group's activities. As cybercrime in a narrow sense was often a necessary preparatory act for cybercrime in a broad sense, several groups were active in both areas.

Table 6: Offline groups entering cybercrime

Offline groups entering cybercrime (Category 1, N = 5)
<p>1 – Spying and interception of data, computer fraud, money laundering (CC.i.n.s.) After having spread malware, the suspects hacked online banking accounts of internet users and spied on their account data. The offenders were then able to carry out unauthorised on-line money transfers to bank accounts of money mules. They withdrew the money from ATMs and transferred the majority of it to the backers abroad.</p>
<p>2 – Fraud, fraudulent failure to supply goods as agreed, spying and interception of data (C.C.i.b.s.) As preparation for further fraud, the offenders established shell companies and hacked suitable (with a good seller reputation) user accounts of an online marketplace. They then used the accounts to deceive dozens of online customers by not delivering ordered and paid goods to the buyers. The majority of the fraudulently attained money was transferred to the backers abroad.</p>
<p>3 – Spying and interception of data, data modification and computer sabotage, fraud, money laundering, handling stolen goods (CC.i.n.s.) Through server hacking and the distribution of malware (including via phishing) the group procured a multitude of complete credit card data which was then used to order high-quality electronics and clothing in online shops. In order to be able to receive the illegally ordered goods, a network of hundreds of parcel mules was necessary. They were acquired through fake 'job offers' via spam emails or on websites especially created for that purpose.</p>
<p>4 – Spying and interception of data, data modification and computer sabotage, fraudulent failure to supply goods as agreed, obtaining goods by fraud, forgery of documents (CC.i.n.s.) The suspects hacked user accounts of an online marketplace in order to offer fictitious goods through them. The buyers of the goods transferred the money to the offenders' bank accounts that mostly had been opened on presentation of falsified foreign passports. The ordered goods were not delivered. The illegally obtained money was then withdrawn or transferred to other bank accounts. Furthermore, the group used stolen credit card numbers to order goods to fake addresses. They also falsified income statements, registration forms from residents' registration offices, and other official forms.</p>

5 – Traffic in human beings for sexual exploitation, procuring (CC.i.b.s.)

Via internet platforms, the offenders made contact with women from the Baltic States and lured them under false pretences to Germany where they were forced to prostitute themselves. This way, the suspects 'employed' several (sometimes involuntarily retained) women illegally. The offenders were responsible for the online advertisement of the women's 'services' as well as for the online contacts with their 'clients'.

Source: IZ 34

Table 7: Offlineborn groups

Offlineborn groups (Category 2, N = 9)
6 – Computer fraud, money laundering (CC.i.n.s.) The suspects infected a huge number of PCs with Trojans and other unknown malware which diverted the aggrieved internet users to nearly identical, but fake online banking websites where they were asked to enter several TAN numbers. Group members abroad were then able to spy on and intercept the bank account login credentials and the TAN numbers. After a couple of days they used the data for unauthorised money transfers from the bank accounts of the deceived internet users to bank accounts of money mules who withdrew the money from ATMs and gave the biggest share to the core group members.
7 – Computer fraud, spying and interception of data, data modification, obtaining goods by fraud (CC.i.n.s.) The offenders infected a large number of PCs with a 'real-time' Trojan in order to spy on online banking data that was then used for unauthorised money transfers. The money mules withdrew the fraudulently transferred money from their bank accounts and divided it between the group members.
8 – Computer fraud, spying and interception of data, forgery of payment cards, money laundering, document forgery (CC.i.n.s.) The offenders spread malware through advertisement banners or through drive-by infections and were able to build several botnets. Their aim was to get direct access to the online banking processes of the victims. In the case of an online money transfer, the malware secretly induced the transfer of a different sum of money to an offenders' account. The money was then withdrawn or online orders were carried out.
9 – Copyright infringement (CC.i.b.S.) The offenders ran a video streaming website with links to illegal copies of films and TV series. High monthly yields were generated amongst other things through advertisement. As opposed to video platforms where users can exchange self-made videos legally, the offenders' streaming website purpose was exclusively to link films and series that were protected by copyright.

10 – Computer fraud (CC.i.n.s.)

Through the use of malware, the offenders were able to intercept login credentials of online banking accounts of a huge number of bank customers. The data was then used for unauthorised online money transfers to bank accounts of money mules, who 'cashed' the money and transferred it to other group members.

11 – Facilitating of illegal entry / migrant smuggling (CC.i.b.s.)

Via several internet platforms the offenders contacted private persons offering 'car rides' from Eastern Europe to Central and Southern Europe and organised the ride of several passengers. Most drivers did not know that their fellow passengers were not allowed to enter the Schengen area and that the transport was illegal and thus that they made themselves liable to prosecution.

12 – Fraud (CC.i.b.s.)

On their websites the group offered services that normally were accessible for free on the internet – e.g. love tests or freeware. In order to access the provided 'services' the internet users needed to enter their personal data into a registration form. Most of them did not realise that the registration led to an annual subscription with costs. In order to make sure that the internet users that had registered would pay, the offenders resorted to demand notes, collection letters, and even opened a call centre where co-offenders urged the users to pay for the (normally free) services.

13 – Spying and interception of data, computer fraud (CC.i.n.s.)

The offenders infected online banking customers' PCs with malware, which allowed them to obtain the login credentials to their banking accounts. The money from these accounts was then used by the offenders to pay in online shops or it was transferred from the compromised accounts to the bank accounts of hired money mules. The mules got a financial remuneration for providing their bank account and for withdrawing the money. Parcel mules collected the ordered goods from offline retail stores.

14 – Fraud, computer fraud (CC.i.b.s.)

By resorting to illegally obtained credit card data (acquired in criminal forums on the internet), the offenders bought several thousand train tickets, which they then sold at a profit to unsuspecting buyers via an online ride-sharing platform.

Source: IZ 34

Table 8: Cyberborn groups

Cyberborn groups (Category 3, N = 4)
<p>15 – Computer fraud, spying and interception of data, falsification of evidential data, document forgery (CC.i.n.s.)</p> <p>With the help of an insider, the offenders spied out the login credentials of employees of a bank and changed bank clients' accounts. This made it possible to initiate money transfers from the clients' accounts to international anonymous debit cards that had been issued under fake identities. After a successful money transfer the offenders were able to pay with the cards in shops or to withdraw money from ATMs.</p>
<p>16 – Trade in narcotic drugs (CC.i.b.s.)</p> <p>The offenders used an internet platform to internationally trade in narcotic drugs (amongst others ecstasy, cocaine and heroin). With the exception of a few personal handovers, the drugs were normally sent by parcel.</p>
<p>17 – Illegal production and distribution of drugs for doping, money laundering (CC.i.b.s.)</p> <p>The offenders ran several dozen websites where the 'customers' were able to order different drugs for doping. The raw material was mostly purchased in Eastern Asia, processed in the Middle East, stored in Western or Southern Europe and from there sent to distributors as well as to end customers in the whole world. The payment for the drugs was transferred to money collectors in the Middle East who withdrew it and sent it to other group members.</p>
<p>18 – Computer sabotage, extortion (CC.i.n.s.)</p> <p>The offenders ran short DDoS attacks on the online shops of several dozen enterprises specialised in e-commerce. The offenders' objective was to disrupt sensitive business processes. They then sent an email to the victims and threatened with the continuation of the attacks unless the companies paid a certain amount in a digital currency.</p>

Source: IZ 34

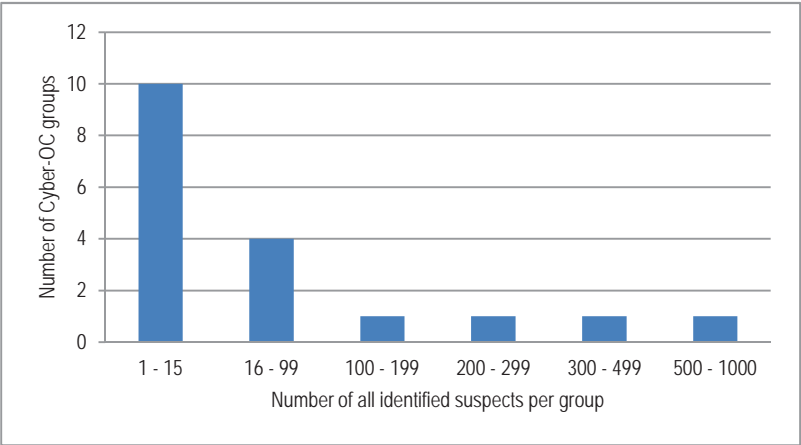
4.5 Characteristics of Cyber-OC suspects

4.5.1 Number

The number of suspects identified in the 18 Cyber-OC groups analysed amounted to at least 1801, of which 124 were core group members (about seven per cent of all suspects). At least 38 suspects (about two per cent of all suspects) exercised a leading role – regardless of which hierarchical level – within a Cyber-OC group.¹¹⁹

The Cyber-OC groups analysed were conspicuous for a wide spread as regards the numbers of their members. For instance, the number of members of a Cyber-OC group ranged from at least five to almost 800 identified suspects. While ten groups consisted of a total of 15 and fewer suspects, four groups had over 100 suspects (see figure 12), resulting in the average size of a Cyber-OC group amounting to approx. 100 identified suspects. The average number of group members attributable to the core of a Cyber-OC group amounted to roughly eight persons. The core groups consisted of at least three to 26 members, with eleven of the 15 groups with information on the core group having fewer than ten core group members.

Figure 12: All identified suspects per group

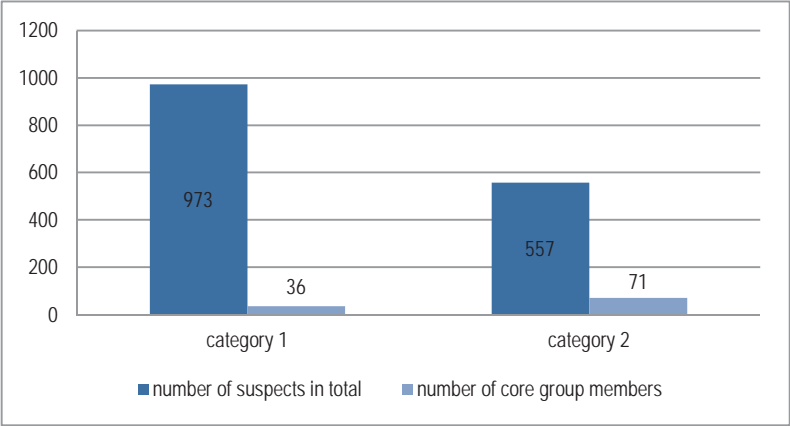


Source: IZ 34

¹¹⁹ Persons considered to be suspects with a leadership function were those who were in charge of the entire Cyber-OC group or at least part of the group, either alone or with others (irrespective of the hierarchy level). Suspects with a leadership function were thus always also members of the core group in question.

Cyber-OC groups in category 1, with an average of approx. 200 suspects, are significantly larger than groups in category 2 (approx. 70 suspects) and category 3 (approx. 40 suspects). With reference to the number of core group members, no major distinctions are discernible between the Cyber-OC group categories. As a result, these figures show that Cyber-OC groups in category 1 and, to a lesser extent, also groups in category 2 have resorted to a high number of supporters (see figure 13). In these cases a relatively small core group was able to create a tightly functioning group structure with a clear distribution of tasks that enabled the criminal activities to proceed ‘smoothly’. For groups in category 3, a similar structure was not identified, which might indicate that the core group members acted relatively autonomously and were not dependent on any extensive ‘support’ from other (partly unknowing) accessories. However, it should be borne in mind here that only in two groups in category 3 was the number of core group members clearly known.

Figure 13: Number of core group members in comparison with total suspects (categories 1 and 2)

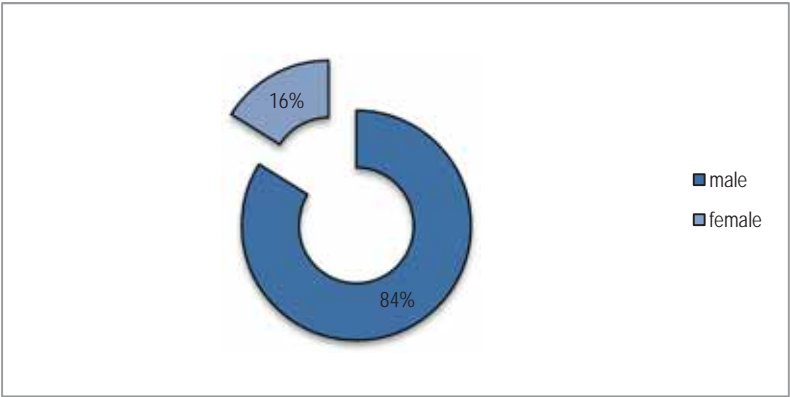


Source: IZ 34

4.5.2 Gender

Gender-related information was available for 270 (approx. 15 per cent) of the total of 1,801 suspects. On that basis it was possible to identify 234 men (84 per cent) and 45 women (16 per cent). Accordingly, roughly five times more men participated in Cyber-OC than women (see figure 15). Taking only the core group members into account, this ratio is even more decisive: 87 male to five female suspects, or approx. 17 times more men than women.

Figure 14: Distribution of gender (all identified suspects)



Source: IZ 34

Contrary to the widespread belief that cybercrime is chiefly dominated by men, the analysis of the suspects in the 18 investigation cases revealed that there certainly are also women who are actively engaged in this field of crime – if only rather in the group periphery than as core group members. Women were engaged in 13 of the 18 Cyber-OC groups – in all five groups in category 1, in seven of the nine groups in category 2 and only in one of the four groups in category 3.

In addition, approx. 16 per cent of the suspects were female. In the case of the core group members, the share of female suspects was substantially lower at approx. five per cent. However, women were only represented in five core groups and assumed a leading role only in two groups.¹²⁰ Accordingly, they are assigned a secondary role in Cyber-OC groups, not only in qualitative but also in quantitative terms.

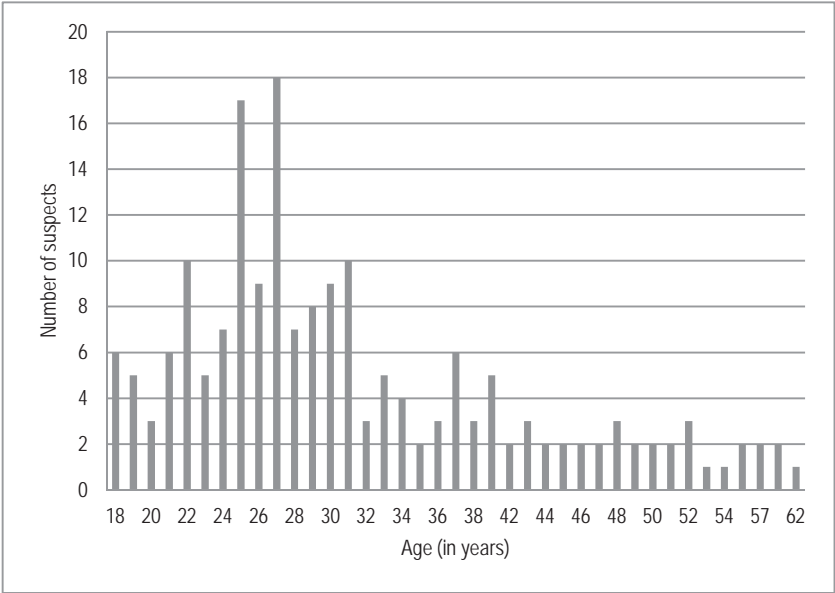
4.5.3 Age

In total, information on the age of up to 185 Cyber-OC suspects (some ten per cent of all suspects) has been collected for the project. On this basis, a Cyber-OC suspect was aged 31.6 years on average, with a wide range existing between the youngest – at 18 – and the oldest suspect – at age 62 (see figure 15). By far the majority of the suspects were younger than 35 years old. Most

¹²⁰ Information on gender was provided for 35 group members with a leading role.

suspects (32 per cent) were aged 25 to 29 years, followed by the 18 to 24-year-olds (23 per cent) and those aged 30 to 34 years (17 per cent).

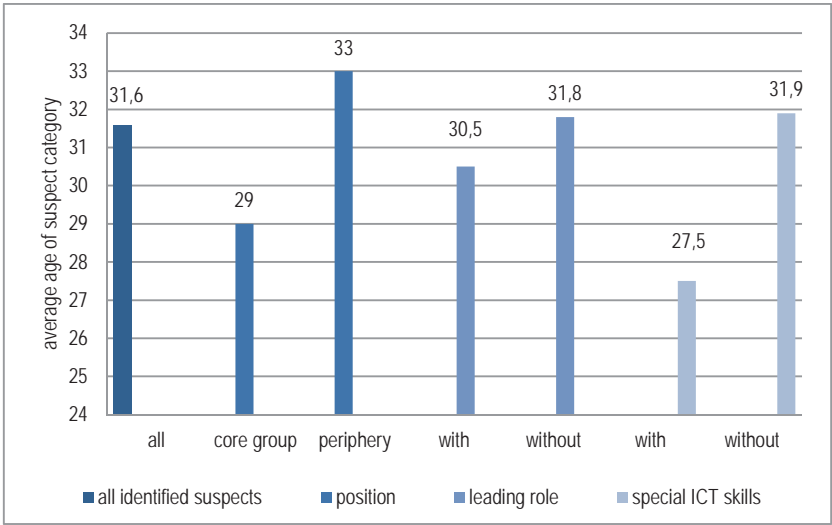
Figure 15: All identified suspects by age



Source: IZ 34

The average age of the 67 core group members with age data was approx. 29 years and amongst those with a leading role with age data the average was 30.5 years. It is notable that core group members on average are considerably younger than suspects from the periphery and that suspects with a leading role within the group are also younger than those without such roles. This shows that a comparatively young age does not preclude a central and leading role within a Cyber-OC group (see figure 16).

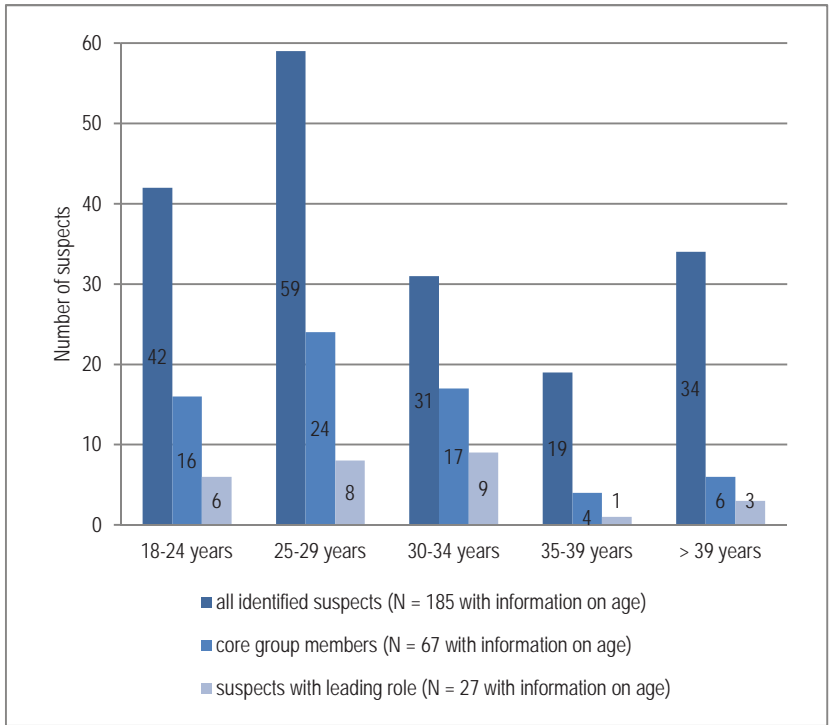
Figure 16: Average age of suspect categories



Source: IZ 34

Cyber-OC suspects aged 40 years or more tended to play a subsidiary role both in quantitative and qualitative terms (assumption of a leading function) (see figure 17). While it was possible to identify suspects who were aged 40 and older in a total of nine Cyber-OC groups (i.e. in every second group), only in two groups did they assume a leading role within the group.

Figure 17: Distribution of suspects according to age classes

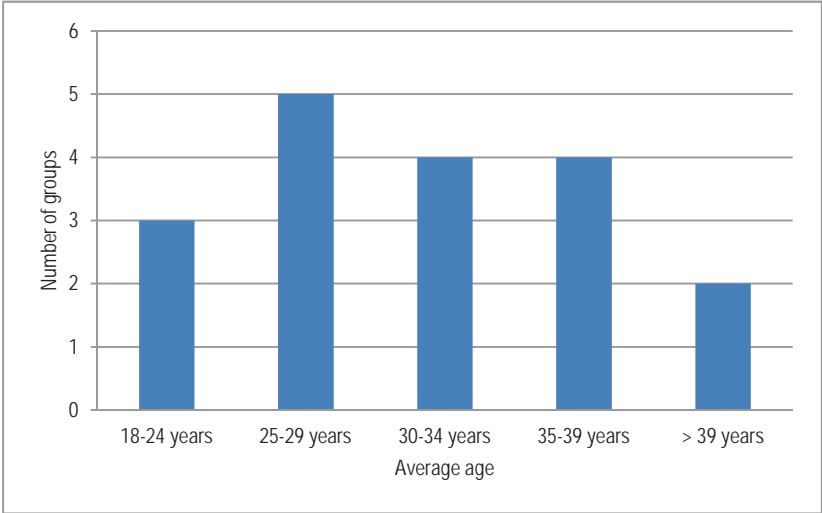


Source: IZ 34

Cyber-OC groups most frequently had an average age of 25 to 29 years (five of 18 Cyber-OC groups), followed by four groups with an average age of 30 to 34 and a further four groups with an average age of 35 to 39 years. Only in three groups did the average age of suspects range from 18 to 24 years; in two groups the average age of all suspects was estimated at approx. 40 years and over. Whereas there were no Cyber-OC groups in category 1 with an average age below 30 years, among the nine groups in category 2 there were six and among the four groups in category 3 there were two. Accordingly, groups in category 1 had a higher age on average (all five groups with an average age between 30 and 39 years) than groups in categories 2 and 3. This difference can be explained by the fact that in addition to the higher average age of their core group members (approx. 27 to 36 years), two out of the five groups in category 1 comprised more than 100 suspects with a lot of supporters of higher age amongst them (see figure 18). All in all, the analysis of the 18 investigation proceedings illustrates that suspects in groups of traditional

OC, for which cybercrime merely represents one of many fields of activity, actually had a higher age in comparison to the suspects belonging to the so-called offlineborn and cyberborn groups.

Figure 18: Average age per group



Source: IZ 34

With reference to all identified suspects, members who belonged to a Cyber-OC group in category 1 were aged 33.5 years on average, meaning they were significantly older than the average Cyber-OC suspect. In contrast, suspects in categories 2 (28.4 years) and 3 (29.4 years) were younger on average. The same is true when comparing the group categories with respect to their core group members. While the average age in relation to all core group members was 29 years, core group members from Cyber-OC groups in category 1 were 31.3 years old, and therefore older. Core group members of categories 2 (28.4 years) and 3 (27.8 years) were younger on average than the average core group member.

4.5.4 Origin

Information for the project evaluation was available for 177 suspects (approx. ten per cent of all suspects) with regard to their nationality or country of birth.

With regard to origin, the results of the analysis give rise to the conclusion that the Cyber-OC suspects predominantly originated from the following countries: Russia and other successor states to the Soviet Union (n = 71; 40 per cent), Germany (n = 68; 38 per cent) and Eastern Europe (n = 15; 8 per cent). Considerably fewer suspects came from the rest of Western, Central and Southern Europe (n = 10; 6 per cent) or from the Middle East (n = 8; 5 per cent). With a few exceptions (n = 5; 3 per cent), namely those from the USA, South Africa, Australia, Pakistan and Afghanistan, no suspects were recorded from the continents of Asia, Australia, the Americas or Africa.

Of the 33 suspects with a leading role with data on their citizenship, over half (n = 17) originated from Russia or another successor state to the Soviet Union and ten were from Germany.

With reference to the nationalities of all identified suspects, the majority of Cyber-OC groups can be designated as heterogeneous since 14 of the 18 groups of suspects were from at least two different countries.

A closer look at the nationalities of only the core group members revealed that only four core groups were heterogeneous, whereas nine were homogeneous.¹²¹ While three out of the nine homogeneous core groups were surrounded by a homogeneous periphery,¹²² five were surrounded by a heterogeneous periphery (see figure 19).¹²³ Of these five Cyber-OC groups whose core group members were of the same origin¹²⁴ and who resorted to supporters of other nationalities, three were included in category 1 and two in category 2. It is conspicuous here that the group core often 'remains in a camp of its own' (i. e. with a homogeneous, mostly foreign origin structure) and that the group periphery is often recruited locally in Germany, making the group as a whole more heterogeneous.

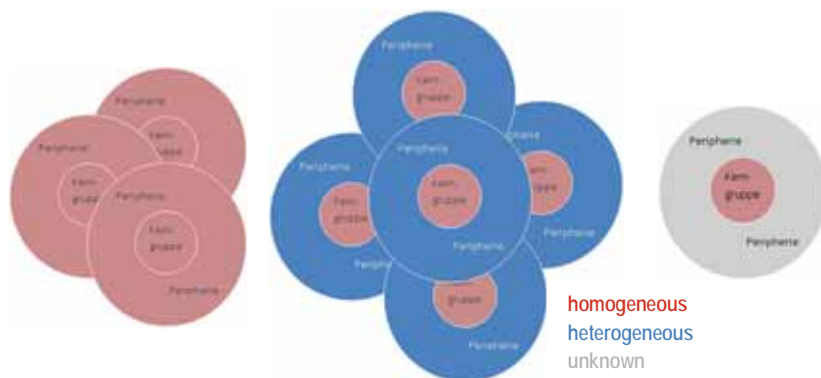
¹²¹ No statements could be made on five core groups with regard to the origin of their members.

¹²² All three groups consisted exclusively of German citizens.

¹²³ For one group with a homogeneous core group the nationalities of the periphery could not be determined.

¹²⁴ Chiefly from Russia or other successor states to the Soviet Union or from Eastern Europe.

Figure 19: Cyber-OC groups with a homogeneous core group (n = 9)¹²⁵



Source: IZ 34

4.5.5 IT skills

Data on special IT skills was available in the respective criminal records for 17 suspects (roughly one per cent of all Cyber-OC suspects).¹²⁶ Whereas five of these suspects acquired these IT skills as part of their studies or vocational training, four suspects learned these skills in their leisure time and with the use of internet forums (on the deep web). Special skills included the preparation and reprogramming of bot networks, the execution of DDoS attacks, the development of one's own malware and the use of sophisticated encryption techniques.

15 of the 17 suspects with special IT skills were members of their respective core group. In two cases they were experts to whom the core group members initially turned within the framework of Crime-as-a-Service. Owing to an increasing permanency of cooperation with them, they were considered part of the group during the project. In addition, nine of them held a leadership function and thus occupied a central role within the respective Cyber-OC group.

¹²⁵ Core groups (Kerngruppe) / peripheries (Peripherie) composed of suspects of the same nationality are shown in red (homogeneity). Those composed of suspects with different nationalities are in blue (heterogeneity).

¹²⁶ As the records evaluated only relatively seldom contained any information on the IT skills of individual suspects, the following information is only meaningful to a limited degree.

While three of the four Cyber-OC groups in category 3 included members with special IT skills, this was only the case in about half the groups in categories 1 (two of five groups) and 2 (five of nine groups).

This shows that several groups also managed to cope without members who had special IT skills. One reason might be the lack of specific data in the respective criminal records. Furthermore, there might also be group-specific reasons: on the one hand, because the criminal activities of the group did not require any special IT skills and on the other hand, the members resorted to specific support by external IT experts or used instructions existing on the internet (Crime-as-a-Service). What is interesting in such cases is whether these IT specialists can be considered to be part of the group. In the German case study, if support services were identified that were unique in nature, these specialists were not counted as part of the group. However, tendencies were identified in the sense that Cyber-OC groups habitually integrated good services on a permanent basis and placed business relations of this kind on a solid, constant footing. Such tendencies are reflected in large amounts of money being diverted on a regular basis to the experts from the criminal profits or the fact that the group turned to them on a 'daily' basis.

4.5.6 Criminal background

It was possible to collect data on a total of 63 suspects (3.5 per cent of all suspects) concerning their criminal background. While no police information was available on 23 of them, 40 suspects had a criminal record. Nearly half of them ($n = 19$) belonged to the respective core group, and roughly one third ($n = 13$) took on a leading role within the group.

Suspects with a criminal past were found in 13 of the 18 Cyber-OC groups: in all five groups in category 1, in six of the nine groups in category 2, and in two of the four groups in category 3. The fact that the groups in the first category comprised members with police records is not surprising as in all five cases, by definition, (traditional) OC groups were involved who extended their activities to cybercrime.

4.5.7 Motivation

For 254 (14 per cent of 1801) suspects, information was provided on the motives for participating in the criminal activities of the Cyber-OC group. The big majority (some 90 per cent, $n = 225$) of the suspects participated in the activities of the Cyber-OC group with the aim of personal financial enrichment.

One Cyber-OC group from category 3 was particularly conspicuous, as for all five group members personal financial enrichment merely played a secondary role. The available records showed that the suspects were primarily interested in the technical challenge, contact with like-minded people, the possibility to compete with others, gaining reputation (prestige-based motive), and the kick experienced in committing crimes.

Moreover, a large number of suspects participated unwittingly in the activities of the Cyber-OC groups. They were misused by core group members e.g. as drivers or money and parcel ‘mules’. While they also pursued the objective of financial enrichment through their actions, they were often not aware that in doing so they were supporting a Cyber-OC group.

4.5.8 Suspects with a leading role

In addition to the findings already specified on suspects playing a leading role within the group, the following is provided as a supplement: 38 suspects (about two per cent) assumed a leading role within the group. On average, at about 30.5 years of age, they were approx. one year younger than the suspects without a leadership function (31.8 years).

The big majority of them by far were male (33 men, compared with only two women) and more than a quarter of them ($n = 9$) had special IT skills. Suspects with a leading role were also conspicuous for an above-average frequency of a criminal background as about every third suspect with a leading role ($n = 13$) had a criminal background, whereas in comparison only about every eighth core group member (15 per cent) had a criminal past.

4.6 Characteristics of Cyber-OC groups

In the course of the evaluation, five groups were able to be assigned to category 1. All of the five groups emerged offline and expanded their criminal activities into the field of cybercrime. Three out of the five groups mainly committed cybercrime in a narrow sense, and two used ICT as tools of crime (cybercrime in a broad sense). A closer examination reveals that this category concerns groups of so-called traditional OC that have expanded into the field of cybercrime.

The nine groups within category 2 show the same characteristics in respect to the place and the reason for their formation. They emerged offline owing to personal acquaintances with the aim of committing cybercrime. Five out of nine groups predominantly committed cybercrime in a narrow sense (e.g. professional computer fraud or spying and interception of data), whereas four

made use of ICT as tools of crime (for instance in cases of trafficking, organised infringements or professional fraud).

According to the group categorisation, the four Cyber-OC groups in category 3 are united by the convergence of the place and the reason for their formation. All four groups emerged from an online environment with the aim of committing cybercrime. Two out of the four groups put their main emphasis on cybercrime in a narrow sense, for instance the development of botnets with the aim of conducting DDoS attacks, spying, intercepting bank account data and making illegal credit transfers. The remaining two Cyber-OC groups mainly committed cybercrime in a broad sense and made use of the internet as a platform to order and sell narcotics or drugs.

4.6.1 Group size

The average size of a Cyber-OC group, calculated from all 18 groups analysed, amounted to 100 suspects (with at least 5 to a maximum of 760 suspects identified).

Category 1

It was possible to assign a total of five groups to this category, with the average total group size (i.e. core group plus periphery) amounting to approx. 200 suspects. The groups in this category are conspicuous for comparatively small group cores and large ‘supporter circles’ (up to approx. 800 suspects).

Category 2

Comprising a total of nine groups, this is the largest category in terms of sheer numbers. The average size of the group as a whole in this regard came to 70 suspects, with the core groups consisting of eight suspects on average. Again, as a rule large peripheries were observed here; some were twice the size of the core groups.

Category 3

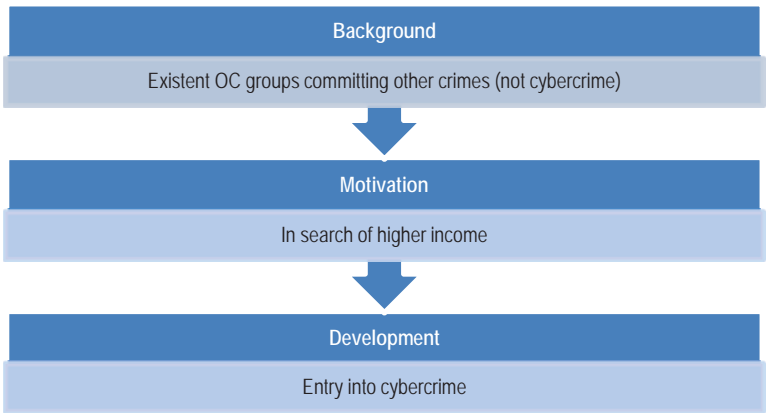
For the total of four cyberborn groups, the size of the group as a whole came to 37 suspects on average. Unlike the groups analysed in categories 1 and 2, in category 3 the peripheries mostly were smaller than the core groups, which implies that cyberborn groups are not dependent on support from numerous additional accomplices.

4.6.2 **Origin, purpose and organised crime relevance**

Category 1

The groups in category 1 originated in an offline context and can be assigned to OC. Committing cybercrimes mostly served to extend their criminal portfolio with the objective of achieving higher profits. The OC relevance of these groups is very high as they practically transferred OC-related commission to cybercrime, operating with a similar, insulated structure and in a commercial manner. Most of the groups in category 1 featured relations to Russian-Eurasian OC, with criminal cooperation also being observed between representatives of outlaw motorcycle gangs and Russian-Eurasian organised crime groups. Striving for profit was the main purpose of criminal collaboration.

Figure 20: Formation process of cyber-entering groups



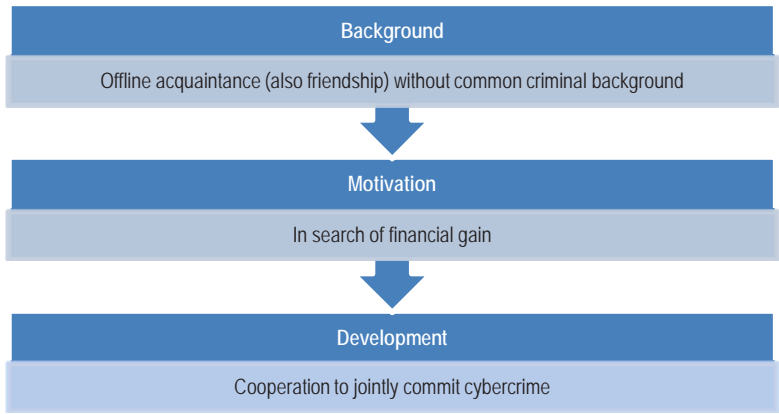
Source: IZ 34

Category 2

Similarly to category 1, the groups here originated in an offline context. Unlike the groups in category 1, which were already criminally active prior to engaging in cybercrime, these groups explicitly joined forces to commit cybercrimes. Another difference in relation to category 1 is that the suspects may have known each other, but they had no previous shared criminal experience. In most cases, the foundations for the formation of groups were based on personal acquaintance (owing to family or friendship connections or common origins). Again, striving for financial enrichment was the main reason for the criminal combination. Groups about which statements could be made on their structure were hierarchical in nature (with three to four levels) oper-

ating conspiratorially and with a division of labour. As in category 1, owing to sophisticated concealment, the police were able to investigate the roles different suspects assumed (e.g. nicknames). However, it was sometimes difficult to clarify the identity of group members behind a particular role, especially when the group members were acting from abroad.

Figure 21: Formation process of offlineborn groups



Source: IZ 34

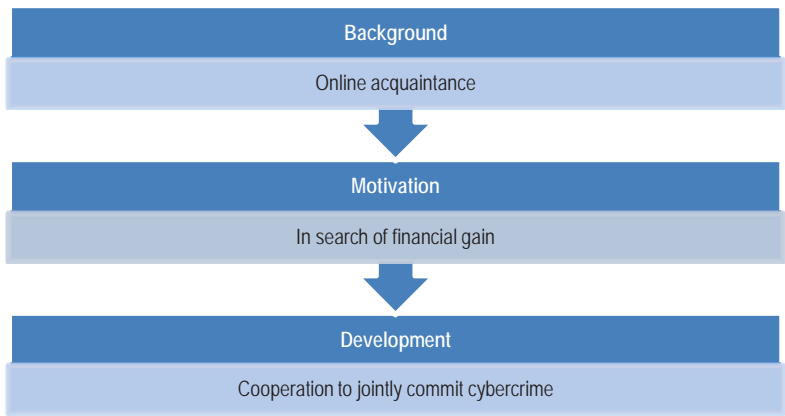
Category 3

Unlike the groups in categories 1 and 2, the suspects here met in an online environment. Accordingly, the origin of the groups was based on contacts on criminal (German) communications and trading platforms of the underground economy and other internet chat rooms. The online acquaintanceship constituted the basis of the criminal associations and ran under the ‘anonymity pledge of encrypted communications’ on the relevant internet platforms. Against expectations, the evaluation showed that maintaining strict anonymity amongst the group members did not represent an irrevocable dictate. Instead, core group members were prepared to disclose personal details to each other or to external supporters. As a result, this created a potential ‘susceptibility to blackmail’ that could serve as a guarantor for group cohesion. As in the case of groups in other categories, again financial enrichment was the driving motivational force behind the criminal acts. Motivation in one of the groups represented a special feature in that financial incentives only played a secondary role. In this case, the main issue was to overcome the technical challenges and a ‘trial of strength’ in competing with ‘kindred spirits’.

The joint commission of crimes and division of labour in doing so was due to the complexity of the steps necessary. Even in those cases in which each of the suspects would basically have been able to commit the various steps independently, the criminal cooperation made the execution of crimes easier and feasible in the first place.

Despite differences in structures and role distributions, all cyberborn groups were conspicuous for commercial, conspiratorial operation under division of labour, which is why the danger potential in such cases is to be considered at a similar level to OC. Even in cases with rather flatter hierarchies (network-like associations with partners almost equal in status) and comparatively less professional behaviour, the companies affected by cyberattacks (DDoS attacks followed by extortion) sustained considerable damage or loss. This makes it clear that damage and danger potential need not necessarily correlate positively with a hierarchical structure.

Figure 22: Formation process of cyberborn groups



Source: IZ 34

4.6.3 Duration of collaboration¹²⁷

In 17 groups, the documents relating to proceedings contained information on the duration of cooperation. On average, a Cyber-OC group managed to exist for one and a half years before it was possible to put a stop to their criminal actions in the course of the investigations.

- Cyber-entering groups – between one and three years; on average one and a half years.
- Offlineborn groups – between half a year and three years; on average just under one and a half years.
- Cyberborn groups – between half a year and four years; on average 21 months.

4.6.4 Group composition

Category 1

In their core, the groups were dominated by foreign nationals; most came from the Slavic-language region. As a rule, the leading positions in Germany were entrusted to ‘fellow countrypersons’. Suspects at the lower execution levels (e.g. financial agents) were mostly German citizens. This constellation, in which a homogeneous core group ‘exploits’ a heterogeneous periphery, tended to be identified in particular in groups of this category. In one group, the homogeneity of the core group was broken by including a few Germans as their membership was most probably considered particularly ‘profitable’ for the group in question.

Category 2

Whereas none of the Cyber-OC groups in category 1 was homogeneous as a whole in terms of the nationalities of suspects, in category 2 there were cases

¹²⁷ In all cases investigated here, collaboration between the suspects came to an end due to the investigation measures. Had the investigation procedures not been initiated, the Cyber-OC groups could accordingly have continued to exist even longer; consequently, these statements are not adequately meaningful to describe the sustainability of the structures identified. Thus, the duration of a group’s collaboration merely shows how long the Cyber-OC group was able to exist until it was destroyed by the investigating authorities. Moreover, it is possible that some Cyber-OC groups were already cooperating with one another covertly prior to the date established for the start of such illegal operations. The duration of collaboration between the Cyber-OC groups in category 1 merely refers to their cybercrime activities and does not extend to include their preceding criminal cooperation.

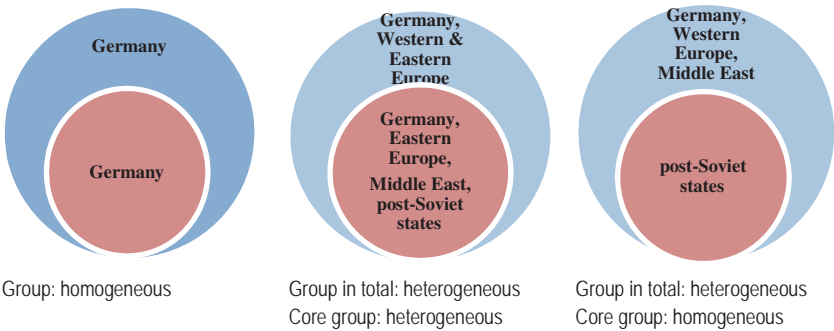
of only suspects of the same nationality (Germans in both cases) cooperating with one another. Two others – as in category 1 – had a homogeneous core that controlled a heterogeneous periphery. However, most of the groups in category 2 had a heterogeneous composition.

Category 3

Only one group was homogeneous (German citizens). The remaining three groups had a heterogeneous character in terms of their composition.

It can be concluded that, particularly in the case of remotely controlled off-line-born groups in categories 1 and 2, there is a structure with a homogeneous group core accompanied by heterogeneous peripheries. Not only in these groups, which were characterised by (remote) control from abroad, but also in the other groups in categories 1 and 2, the shared ethnic background played a central part in the group’s origination, in the successful execution of the criminal activities and in the associated trust necessary. An organisation model of this kind, characterised by control from abroad, was not identified in category 3. What is more, the common ethnic background does not appear to play a particular role in the origin of the group or its criminal activities.

Figure 23: Composition of core groups and peripheries of selected groups



Source: IZ 34

4.6.5 Group structure

Category 1

The majority of OC groups that became involved in cybercrime represented a smoothly functioning organisation model remotely controlled from abroad in which strict hierarchies at several levels became visible along with a clear distribution of roles. As a rule, the groups controlled from abroad committed

cybercrime in a narrow sense, with a relatively small group core including and coordinating a number of supported persons in the group periphery in carrying out the criminal offence. It can safely be assumed that the master-minds abroad are 'expanding' in line with the described model but not only in Germany.

Figure 24: Example of hierarchic group structure



Source: IZ 34

Category 2

All groups in this category, with one exception (in which core group members were not identified) had a hierarchical structure. The phenomenon of 'remote control' identified in category 1 also manifested itself here, with most of the suspects operating abroad being located in the Russian-speaking region. The groups also had a similar structure with a high degree of organisation, clear division of labour, several hierarchical levels and strong resistance to infiltration from inside and outside. Like the 'remotely controlled groups' in category 1, the similarly structured groups here are also beginning to commit primarily cybercrimes in a narrow sense. It is conspicuous that such OC-like structures are also being established by perpetrators who, unlike those of the groups in category 1, did not have a common previous criminal history, let alone OC experience of any kind.

In addition to the described model of groups remotely controlled from abroad, in category 2 groups with different structures became visible that committed cybercrimes in a broad sense. This illustrated how the deployment of ICT as instruments of crime in combination with the effectiveness of an OC-like organisational structure can successfully lead to criminal enrichment. In terms of their structure, these groups were similar to online companies.

In only two cases was it possible to refer to the group structure as rather flat in comparison with the other hierarchically structured groups. In this context, the focal point of collaboration was not on the establishment and maintenance of a certain command chain, but on the fundamental consensus or arrangement to proceed with the division of labour, which is reflected e.g. in the percentage-based sharing of the criminal proceeds. The various roles were able to be differentiated less clearly in comparison to other groups. Nevertheless, three group levels were identifiable: level 1 – leader and source of ideas for the group; level 2 – ‘right-hand-man’ or closest confidant of the initiator and level 3 – money mules. In order to carry out specific tasks, the suspects relied on the services of ‘hackers’ outside the group. Thus the conclusion can be drawn that Cyber-OC groups can operate ‘successfully’, relying on the division of labour and a high degree of resistance to infiltration from inside and outside even without strict hierarchical structures and a fixed distribution of roles.

Category 3

Unlike the first two categories, in this case (with one exception) strict hierarchical structures are lacking. The majority of the cyberborn groups were organised in jointly operating networks of almost equally privileged ‘partners’, with the division of labour depending on expertise, experience and access to technical and logistical instruments of crime. Owing to the tangible and intangible loss or damage, the automated generation of victims, the modus operandi and mechanisms for resistance to infiltration applied, such networks cannot be considered to be less dangerous than the other groups analysed. On the contrary, such a group that originated online can proceed in an extremely well-planned manner and with division of labour and can display an expedient flexibility that in a certain sense allows criminal acts to be committed ‘irrespective of any persons’.

In addition, the remote control identified in the other categories was not discernible here in a comparable form. The suspects joined forces via the internet and carried out all the steps of the criminal offence in a complex way using division of labour and the relevant abilities themselves, without being reliant on large circles of supporters.

In addition, an analytical observation of the organisational structure of the cyberborn groups indicates that strict hierarchies with vertical command chains are not a prerequisite for the successful organisation and execution of technically complex criminal offences against ICT.

4.6.6 Trust and sanction mechanisms

The evaluation shows that groups from category 1 used more ‘traditional’ off-line trust sanction mechanisms. In category 2 a mix of offline and online (technical) tool was used, while the groups from category 3 applied mostly online controls and sanctions.

The detailed results of the evaluation on this characteristic are determined only for police use and for this reason cannot be further explained here.

4.6.7 Summary Cyber-OC groups

Table 9: Characteristics of Cyber-OC groups – summary

Characteristics	Category 1 Offline groups entering cybercrime (5 groups)	Category 2 Offlineborn groups (9 groups)	Category 3 Cyberborn groups (4 groups)
Group size	Ø = 200 core < periphery	Ø = 70 core < periphery	Ø = 37 core > periphery
Origin	group formed to commit offline crimes (not cybercrime), then enters cybercrime	group forms offline to commit cybercrime	group forms online to commit cybercrime
Crimes	- computer integrity crimes - computer-assisted crimes - online illicit market-places	- computer integrity crimes - computer-assisted crimes - computer content crimes - online illicit market-places	- computer integrity crimes - computer-assisted crimes - online illicit market-places
Motive	pursuit of profit	pursuit of profit	pursuit of profit, technical challenge
Duration	Ø = 1 year 6 months	Ø = 1 year 6 months	Ø = 1 year 9 months
Composition	- group as a whole: all groups heterogeneous - core/periphery: most groups with homogeneous core leading heterogeneous periphery	- group as a whole: most groups heterogeneous - core/periphery: few groups with homogeneous core leading heterogeneous periphery	- group as a whole: most groups heterogeneous - core/periphery: no group with homogeneous core leading heterogeneous periphery

Characteristics	Category 1 Offline groups entering cybercrime (5 groups)	Category 2 Offlineborn groups (9 groups)	Category 3 Cyberborn groups (4 groups)
Group structure	- strictly hierarchical with clear division of roles - leadership abroad - high level of concealment	- mostly hierarchical, mostly clear division of roles - often leadership abroad - high level of concealment	- mostly network-like, with rather flat hierarchies and often flexible division of roles - rarely leadership abroad - high level of concealment
Trust and sanctions	based on 'traditional' offline mechanisms	based on a mix of offline and online (technical) mechanisms	mostly based on online (technical) mechanisms

Source: IZ 34

4.7 Activities and modi operandi in the field of Cyber-OC

Many Cyber-OC groups were involved not only in one but simultaneously in several fields of crime and committed cybercrimes in a narrow and in a broad sense. To some, the commission of cybercrimes in a narrow sense was a necessary basis for successfully carrying out additional criminal acts. To other Cyber-OC groups, cybercrime in a broad sense occurred in parallel with their original criminal activities – this accordingly augmented the group's criminal repertoire – and represented an extra source of 'revenue' for the group. In preparation for cybercrime in a narrow sense, other groups initially had to commit other crimes, such as fraud, theft, or using false information to open accounts or to found enterprises.

As already described, many Cyber-OC groups (particularly in category 1 but also category 2) were conspicuous for the fact that their 'masterminds' were located abroad. ICT facilitated logistics and communications with accomplices in Germany to a great extent. On a number of occasions, innocent persons were drawn into the criminal activities of Cyber-OC groups (e.g. private providers of cross-border car rides offered on the internet). Without their participation and/or misuse, the groups would not have been able to carry out the criminal acts (to the same extent).

What was typical of all groups of perpetrators was that they frequently operated throughout Europe and their deeds could only be carried out with the division of labour and partly by using specialist expertise. In addition, it was observed that criminal groups exchanged instruments of crime (malware) be-

tween one another. In the course of the investigations against a Russian-language dominated group, it was identified that good relations were in place between groups operating in the same ‘field of business’ (e.g. phishing).

Conspiratorial behaviour was also typical of all Cyber-OC groups. As a rule, the execution of criminal acts focused on using sustainably designed criminal acts to generate sizable profits at the expense of numerous victims: for instance, about 100,000 PCs infected with a real-time Trojan; several tens of thousands of defrauded internet users; several dozen online enterprises impacted by DDoS attacks.

In summary, it can be said that many Cyber-OC groups, both offlineborn and cyberborn, covered a wide range of criminal acts and were in a position to commit technically sophisticated crimes. All Cyber-OC groups analysed operated with a division of labour and in a conspiratorial manner. It was typical for the majority of offlineborn groups that their ‘masterminds’ were located abroad, with ICT, amongst other factors, facilitating the ‘smooth’ functioning of the structures in Germany.

4.8 Damage of Cyber-OC

The threat potential that emerges from Cyber-OC groups is diverse and holds serious risks for society, the economy and individuals.

Given the prominent role of ICT in daily life, the overall risks of Cyber-OC attacks are hardly measurable. As a consequence, presenting the threat potential by solely referring to financial damage would be biased and misleading as this would not show the real or entire picture. Moreover, while there was relatively little information on financial damage, the files of the analysed cases gave information on the number of hacked online accounts and infected PCs and the volume of illegally used storage space.

It needs to be stressed that the quantitative and qualitative damage dimensions in the field of Cyber-OC have not yet been sufficiently described and that they are still subject to wide discussion. The diverse damage forms existent in the field of Cyber-OC also appeared in this project as immaterial forms of damage could be identified in all cases.

4.8.1 Material damage

Details on the financial damage caused by Cyber-OC groups were available in the majority of the cases. The total financial damage caused by the Cyber-OC groups in the sample amounted to approx. 115 million euros.¹²⁸

In all group categories, especially in the groups within categories 1 and 2, the financial damage was mainly caused by the fact that various amounts of money were stolen from the online bank accounts of private internet users. In a lot of cases, Cyber-OC groups gained access to the money through the spread of malware, which gave them access to the online bank accounts of the victimised internet user and further enabled them to conduct illegal transactions and withdrawals. Moreover, various groups also used previously stolen credit card data which they purchased on the internet. With the aid of these data records they paid for e.g. goods and train tickets or used money mules who withdrew the money at ATMs. Generally, the financial damage due to illegal online transfers was detected and covered by the respective banks. In some cases the money mules were required to pay back the withdrawn money.

Internet users were also harmed by ‘fraudulent failure to supply goods as agreed’ offences in which the perpetrators for instance did not deliver the goods ordered and paid for via the internet by the victim.

‘Obtaining goods by fraud’ offences were another way that financial damage was caused. An example here might be the online payment of goods or services with stolen credit card data. Often, the banks realised the illegal use of the credit cards only after the goods had already been delivered to the offenders whereupon, in many cases, the banks then reversed the amount of money back to the credit card owner’s account. As a consequence the aggrieved parties were the online shops, the credit card processors and the banks handing out the cards.

In one case enterprises specialising in online commerce experienced short DDoS attacks and were then threatened with the prolonged conducting of DDoS attacks that would lead to the complete interruption of their websites if they did not pay a certain amount of money. The financial damage was calcu-

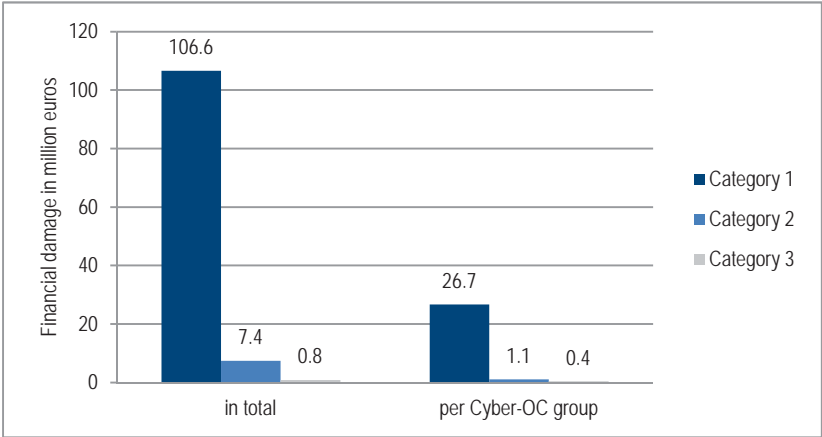
¹²⁸ For the herein calculated amount of financial damage, numbers from the file records were taken. Frequently, these numbers were minimum values. In some cases the total damage evaluated was composed of, on the one hand, the threatened damage (attempted, but not accomplished) and on the other hand the actual financial loss. In order to calculate the amount of damage caused by Cyber-OC, only the actual financial loss was considered, if possible. As the evaluated Cyber-OC cases only account for a subset of all Cyber-OC preliminary proceedings in Germany, the calculated damage does not mirror the actual damage in the crime field of Cyber-OC.

lated according to partly transferred payments of ‘protection money’ and according to high losses in income in connection with the breakdown of online shops lasting for several days.

Financial damage further arose because of the Cyber-OC groups offering product copies or streaming services on deep web forums, which simultaneously prevented the producer of these products or films from generating vast amounts of financial income.

The highest financial losses in total as well as per Cyber-OC group can be allocated to category 1. These Cyber-OC groups correspondingly caused losses of approx. 26.7 million euros on average. The average loss caused by categories 2 and 3 with approx. 1.1 and 0.4 million euros respectively is 24 to 67 times lower than in category 1 (see figure 25).

Figure 25: Financial damage in the analysed Cyber-OC cases



Source: IZ 34

Among other things, the high value within category 1 is retraceable to the fact that two Cyber-OC groups in this category caused above average losses, namely six and 100 million euros. The high level of damage in category 1 might also be explained by the above average size of Cyber-OC groups within this category – on average they are three times bigger than category 2 Cyber-OC groups and more than five times bigger than category 3 groups. But various groups in category 2 also showed an above average amount of damage.

The findings of the file analysis show that traditional OC groups are also very dangerous in an online environment as the highest financial damage was caused by category 1 groups that committed cybercrime in a narrow sense. This illustrates that by committing ‘new’ and technically complex offences

(cybercrime in a narrow sense) traditional OC groups entered a very profitable crime field.

Some Cyber-OC groups revealed high values of threatened damage in comparison to the actual damage. For instance one group in category 2 caused actual fraud losses amounting to 4.5 million euros, while the threatened damage was estimated at around 48.5 million euros in total. Moreover, one group in category 3 caused an actual damage of 310,000 euros while the threatened damage was estimated at 3 to 5 million euros.

This discrepancy between the actual damage and the threatened damage shows that Cyber-OC groups were not always ‘successful’ with their criminal activities. However, with the financial potential damage they could have caused being so high, the dangerousness of Cyber-OC groups becomes even more evident. In several cases their criminal actions were merely able to be prevented by the involvement of banks (cancellation or reverse of illegal money transfers). Such cases did not cause an actual financial loss per se for the aggrieved bank account owner, however, it can be assumed that this attempted fraud caused non-negligible immaterial damage such as, for instance, the loss of trust of bank customers using online banking.

4.8.2 Immaterial damage

In all 18 cases immaterial damage was detectable (see table 10).

Table 10: Immaterial damage caused by Cyber-OC groups

Damage	Category 1 n = 5	Category 2 n = 9	Category 3 n = 4
Health damage	no	no	yes (2 groups)
Loss of trust in IT security (e.g. during online banking and shopping)	yes (4 groups)	yes (6 groups)	no
Loss of trust in banks	no	yes (1 group)	yes (1 group)
Loss of trust in security and reliability of online services and social networks	no	yes (2 groups)	no
Damage to someone’s reputation and credibility	no	yes (2 groups)	yes (2 groups)
Copyright infringement	no	yes (1 group)	no
Non-financial damage of perpetrators within the periphery and of further suspects	yes (2 groups)	yes (4 groups)	no

Source: IZ 34

Health damage was only traceable within groups from category 3. They sold narcotics, including heroin which is commonly known to be an extremely dangerous drug, and thus jeopardised 'public health'. The second case revealed that the 'customers' who were supplied by the Cyber-OC group with anabolic substances regularly complained of health issues resulting from taking the drugs in question.

Another kind of damage that emerges because of Cyber-OC groups is related to loss of trust. Internet users' trust in online monetary transactions or in security with regard to online shopping was damaged by four out of the five groups in category 1 and by six out of the nine groups in category 2. This damage was not detected for groups in category 3.

Furthermore, Cyber-OC groups lead to a loss of trust of internet users as their criminal activities induced online banking customers to doubt the ability of their banks to sufficiently protect them from hacker attacks and internal perpetrators (in groups in categories 2 and 3). Moreover, the trust in the reliability of online services and social networks is undermined when e.g. a Cyber-OC group misuses unknowing drivers for trafficking human beings or when people use supposedly free online products and afterwards are 'forced' to pay for them (both times one group in category 2).

Various times Cyber-OC groups carried out activities that led to a loss of image or reputation. The latter always appears, to a certain degree, in connection with the aforementioned loss of trust. In some cases this appears to be of further importance: two groups in category 2 committed fraud, which led to a damaged reputation in one case for a transportation company and in the other case for the producer of freeware for which one Cyber-OC group demanded payments on their website. Additionally, two groups in category 3 caused a damaged reputation in one case for a bank and in the other case for the online shops that broke down for several days because of DDoS attacks.

One group in category 2, by making series and films accessible for free, caused 'systematic damage' to the film and series market and to compliance with copyright.

One last dimension refers to damage that affects group members (primarily from the periphery) or other people who were not part of the group but were 'used' by it. The (unconscious) support of the activities of the core group led in various cases to negative consequences for the suspects within the periphery such as an increase in social pressure and their social exclusion (criminal investigations, insecurity, high debts). In about every second group in categories 1 and 2 such forms of damage were identifiable. Groups in category 3 did not show this dimension of damage. Examples are money mules, drivers, parcel mules, etc., who have been appointed by the core group members

sometimes under pressure (threatening/blackmailing), under false promises (riskless incomes), with false information (on illegality or background) or under the exploitation of emergencies (drug addicts). Often without knowing it, they took the much higher risk of being caught and of negative consequences with regard to their creditworthiness. The negative consequences were kept secret or were underplayed by the group: the suspects of the periphery who were informed about the illegal character of their actions were promised risk-free income by the core group members; suspects who unconsciously participated were mostly not informed about the illegal background.

In one case in category 1, the core group members convinced people via seemingly legal job contracts to unknowingly participate as parcel mules for the group. The parcel mules were damaged in two ways: on the one hand, they did not receive the promised monthly 'salary' from the core group members and, on the other hand, the owners of the credit cards that were used to illegally buy the goods online brought charges against the parcel mules.

Another Cyber-OC group in category 1 lured women to Germany under false premises where, owing to threats and physical violence, they were forced to prostitute themselves. Furthermore, they were put in a position of dependency (through the removal of passport documents and through 'debts' they had to pay) and advantage was taken of their emergency situation (they were generally not able to speak German, etc.).

One Cyber-OC group in category 2 arranged passengers for drivers and withheld the information that these passengers were refugees who did not possess visas for the Schengen area. By taking the passengers with them, the drivers made themselves liable for trafficking human beings. The negative legal consequences for the drivers were accepted by the group. Simultaneously, the group exploited the emergency situation of the refugees by claiming high prices for the arrangement. In another case in category 2 the core group members appointed people as 'managers' of their companies of whom they knew that they would not be mentally capable of understanding the impact of their actions. For example, one of these supporters had difficulty reading and writing and did not understand what the company and the position as a manager really involved.

There were also cases in category 2 where the Cyber-OC group deliberately accepted damage to people who were only indirectly involved in their activities: the purchasers of the seemingly official online train tickets were checked by the train staff at their departure and destination and their personal data was then collected by police officers.

Therefore, similarly to the presented damage dimensions caused by Cyber-OC groups, the victims of Cyber-OC groups are also diverse – they can be

private internet users, online networks, banks, companies (with and without online shops).

In summary, the total financial damage within the 13 cases containing information on this adds up to about 115 million euros. However, the validity of this amount is strictly limited, owing to the aforementioned methodological reasons and various means of concealment.

The actual threat potential arising from Cyber-OC is high, owing to the cumulative nature of the phenomenon (the conjunction of the two crime fields of organised crime and cybercrime), and because of the essential role of ICT in everyday life. Nonetheless, further discussion that might lead to better grounded and more palpable results is needed.

It became evident that the damage caused by Cyber-OC groups was primarily of a financial nature, but it encompasses complex immaterial dimensions, too.

4.9 Investigative measures in the analysed Cyber-OC cases

The information with regard to the initiation and conducting of the investigations within the crime area of Cyber-OC contained in the investigation files was taken into consideration as well. In this process, the judicial measures employed, along with their effectiveness for elucidating the crime, were analysed with the aim of identifying the core challenges for criminal prosecution and developing an overview regarding ‘best practices’.

In the majority of the cases the investigations were started after complaints were filed to the police. The reasons were mostly connected to the abuse of bank accounts, stolen online identities, missing payments of items ordered online, hacked or manipulated PCs or extortion emails. In some cases the investigations were launched because of complaints by third parties (e.g. banks) and in other cases the law enforcement authorities started the investigations as a result of control actions conducted.

With reference to the investigations, the law enforcement agencies applied a wide range of investigation tactics which mostly consisted of a mixture of standard measures and covert investigations. For instance the measures ranged from searching flats and business premises, searching for and securing dactyloscopic traces, measures regarding asset recovery, evaluating communication data, evaluating data carriers, monitoring telecommunications, observations and the usage of undercover investigators, national and international cooperation between the law enforcement agencies and with the private sector.

The main findings with regard to the effectiveness of the investigative measures used in the analysed investigations display the following challenges:

- A lack of legal regulation regarding telecommunication data retention at the time when the investigations in the analysed cases were carried out.
- Enormous data volumes in diverse languages as well as various encryption methods used by the suspects.
- Complexity of suspect structures, which makes it harder for investigators to recognise connections between crimes and/or suspects, especially when the groups acted internationally.
- International judicial cooperation as well as with non-governmental actors was often challenging.

The following best practices from the analysed investigations can be stated:

- The international exchange of information between law enforcement authorities and requests for judicial assistance and JITs were successful in many cases.
- Broad internal cooperation amongst different units often led to significant success.
- Diverse monitoring measures were successful, especially when it came to recognising the roles played by the different suspects within the group.

5 Concluding remarks for Germany

5.1 Answers to the research questions

For correct classification of the present study findings, it should be repeated at this point that these relate to the cases evaluated and do not offer a basis for generalisations or ‘one-to-one’ transfers to similar current or future forms of crime. Instead, the present study represents an explorative investigation that is aimed at facilitating insights for the first time into the characteristics of the complex phenomenon of Cyber-OC.

The study shows first of all that there are manifestations of Cyber-OC in Germany – in accordance with the working definition and the inquiries made on this basis. At the same time, it becomes clear that combating the phenomenon throughout Germany plays an important part in police work and tasks. These

are investigations into almost all crime fields, in which criminal acts are committed both against and also by means of ICT.

With regard to the research questions, it can be noted that Cyber-OC according to the understanding of the project comprises the commission of cybercrime by criminal groups on the one hand and the organised commission of cybercrime on the other.

The second research question, namely whether OC groups are involved in cybercrime, what criminal acts they commit and the effects of the internet on OC structures, can be answered as follows:

- The present evaluation findings support the assumption that criminal groups existing in Germany – amongst others, so-called ‘traditional OC groups’ – have entered the field of cybercrime.
- Moreover, contrary to widespread expectations that OC groups would sooner tend to commit cybercrime in a broad sense (i. e. using ICT as instruments of crime to carry out criminal offences considered to be typical), it was established in the course of the project that they certainly are in a position to carry out technically sophisticated criminal acts from the spectrum of cybercrime in a narrow sense. It became clear in several examples that they themselves have members with extensive IT expertise. In a few cases, these groups made use of Crime-as-a-Service offers. It can thus be documented that criminal groups in search of higher profits with a low risk of discovery succeeded in extending their original ‘criminal portfolio’ – such as illegal narcotics trading, illegal international motor vehicle trading, human trafficking, banking and loan fraud, money laundering as well as theft and shoplifting – to include criminal acts in the field of cybercrime in a narrow sense.
- In the case of Cyber-OC groups that originated offline (i. e. categories 1 and 2), a criminal organisation model remotely controlled from abroad was identified, characterised by strict hierarchies, clear role distributions and high resistance to infiltration from inside and outside. In these cases, the ‘masterminds’ operated from abroad and mostly left the management up to ‘trustworthy’ fellow countrypersons in Germany.
- The majority of these remotely controlled groups predominantly committed cybercrimes in a narrow sense, which indicates that this model is best suited to criminal acts that require technically complex procedures but hardly any physical contact.

- Depending on the satisfaction with the criminal services provided by hackers outside the group, Crime-as-a-Service can certainly become a permanent feature beyond a specific purchase and be converted into a long-term cooperative venture that additionally results in the distribution of the criminal proceeds. In such cases, the IT experts were considered to be part of the Cyber-OC groups owing to their regular collaboration. The evaluation for Germany showed that there were instances of Cyber-OC groups exchanging instruments of crime (e.g. malware). To what extent providers of Crime-as-a-Service actually served ‘several groups’ did not emerge from the German case study, however. In contrast, the findings of the project partners in the Netherlands and Sweden indicate that, in the course of their evaluations, it was possible to observe such multiple cooperative ventures between groups and providers of criminal services.
- As far as the use of criminal IT services outside the group is concerned, the study revealed that even technology-orientated groups have resorted to Crime-as-a-Service.

The question as to whether cybercrime can be committed in an organised form can be answered in the affirmative according to the project findings since:

- In the cases evaluated, cybercrime – irrespective of whether in a broad or narrow sense – was committed with a distribution of labour and a long-term orientation.
- In addition, the results show that cyberborn groups do not necessarily commit cybercrimes in a narrow sense. Two of the four cyberborn groups used ICT to be able to commit traditional crimes (in both cases, illegal trading in narcotics or pharmaceuticals). In the process, the internet not only facilitated their entry into this field of crime, it also gave them access to a global sales market and the associated high earnings.
- As a rule, the organised execution of cybercrime presupposes a close relationship between online and offline criminal acts. This finding was identified in multiple cases, in particular where criminal acts were committed against computer systems in combination with additional crimes in the real world (e.g. hacking of personal data, followed by fraudulent withdrawal of cash). Accordingly, the purely online-supported nature of cybercrime in a narrow sense is thus restricted when the groups were dependent on acting offline as well.
- On account of the project findings, the last research question – Does the internet offer the offenders ‘windows of opportunity’ to develop new, ille-

gal business models and develop additional criminal sources of income? – can likewise be answered in the affirmative. The project findings clearly show that the internet and ICT as a whole simplify the commission of conventional crimes, extend their reach and offer many and various concealment opportunities. An additional factor is that the commission of cybercrimes in a narrow sense constituted a necessary basis for the successful commission of additional crimes or represented an additional source of income when committed in parallel with the original criminal activities of cyber-entering groups.

5.2 Key findings of the German case study

Anonymity, encrypted communications (entailing a perceived reduction of the risk of discovery), but also a diverse range of illegal goods, malware and hacked online identities attract criminals on the lookout for higher profits to commit cybercrime. What happens when ‘experienced’ criminal groups take advantage of these opportunities, and how dangerous can associations or networks of ‘cybercriminals’ actually be? In search of answers to these and other questions, the BKA launched the project ‘Cyber-OC – Scope and manifestations in selected EU member states’.

The project findings indicate that OC groups in Germany have meanwhile entered the field of cybercrime. Not only do they use the internet as an instrument of crime, they are also able to commit sophisticated crimes within the spectrum of cybercrime in a narrow sense.

For cyberborn groups, nationality plays a subordinate role. What is more important is the expertise of the group members and their access to ‘valuable’ technical and logistical instruments of crime, (insider) information and certain online forums. In contrast, for groups formed in the offline world (category 1: cyber-entering groups and category 2: offlineborn groups), the origin and cultural socialisation represent central elements in fostering group coherence. For instance, this difference is reflected in the fact that in cyber-entering and offlineborn groups, key tasks on-site are assigned to ‘fellow countrypersons’, while accomplices of other nationalities (‘local staff’) assume less important and even ‘vulnerable’ roles.

Unlike cyber-entering and offlineborn groups, cyberborn groups less frequently need supporters and, if they do, fewer supporters intended to contribute towards ‘finalising’ cybercrimes by committing other crimes in the real world. This reduces the visibility of cyberborn groups as they generally have fewer connections to the offline world (e.g. they were found to deploy fewer ‘mules’ or ‘solicitors’ and ‘companions’).

In contrast to cyber-entering and offlineborn groups, strict hierarchies in cyberborn groups (in particular those that commit cybercrime in a narrow sense) are fairly rare. Instead, such groups are organised as networks operating with shared resources. The advantage of such a structure is the maintenance of a certain ‘personnel-related flexibility’ that allows suspects to be replaced at random without the execution of the crime being impaired in any way.

And again, unlike offline formed groups (categories 1 and 2), traditional trust-building mechanisms and sanction measures play a subordinate role in cyberborn groups. While knowing someone personally is no prerequisite for a criminal association, in the course of the criminal activities of cyberborn groups this may be strived for as a weighty trust guarantor for continuing or ‘intensifying’ criminal acts (gradually dispensing with the need for virtual anonymity). For control and sanction purposes electronic mechanisms were used.

A hierarchical structure is no prerequisite for the successful commission of technically complex crimes, which means that a network-like cyberborn group that operates with a division of labour and skills is no less dangerous than a group that is established in a hierarchical, OC-like fashion.

Acknowledgements

The elaboration of the German case study was supported by: Heike Bruhn, Nadine Kunze and Julia Weber. Besides, during this project, the researchers had input of several people. Especially we would like to thank all the analysts and investigators from the police services at the federal and state level for their essential support.

6 References

- Bundeskriminalamt (BKA) 2013: Organisierte Kriminalität – Bundeslagebild 2013.
- Bundeskriminalamt (BKA) 2013b: Cybercrime – Bundeslagebild 2013.
- Bundeskriminalamt (BKA) (2014), Polizeiliche Kriminalstatistik Bundesrepublik Deutschland – Jahrbuch 2013. Wiesbaden: Bundeskriminalamt.
- Bundeskriminalamt (BKA) (2014a), Organised Crime – National Situation Report 2014. URL: http://www.bka.de/nn_194550/EN/SubjectsAZ-/OrganisedCrime/organisedCrime__node.html?__nnn=true (accessed on 09.03.2016).
- Bundeskriminalamt (BKA) (2014b): Bekämpfung der Cybercrime aus Sicht des BKA. URL: <http://www.bafin.de/SharedDocs/Downloads/DE-/Ver->

- anstellung/dl_141009_it_sicherheit_vortrag_kraus_cybercrime.pdf?__blob=publicationFile&v=4 (accessed on 09.03.2016).
- Bundeskriminalamt (BKA) (2014c) Cybercrime Bundeslagebild 2014. URL: http://www.bka.de/nn_233866/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrime__node.html?__nnn=true (accessed on 11.03.2016).
- Bundeskriminalamt (BKA) 2014d: Organisierte Kriminalität – Bundeslagebild 2014.
- Bundeskriminalamt (BKA) (2016), The Bundeskriminalamt as a Central Agency. URL: http://www.bka.de/nn_195530/EN/TheBKA/Tasks-/CentralAgency/centralAgency__node.html?__nnn=true (accessed on 09.03.2016).
- Bundesministerium des Innern (BMI) (2016), Cyberkriminalität. URL: http://www.bmi.bund.de/-/DE/Themen/Sicherheit/IT-Cybersicherheit/cyberkriminalitaet/cyberkriminalitaet_node.html (accessed on 11.03.2016).
- Council of the European Union 1997: Doc. 6204/2/97. EnfoPol 35 rev. 2, adopted by the Council on 21 April 1997.
- Council of Europe (2001), Convention on Cybercrime. URL: <http://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561>
- Groß, Hermann (2008): 'Deutsche Länderpolizeien'. [online] <http://www.bpb.de/apuz/-/30826/deutsche-laenderpolizeien?p=0> (accessed on 09.03.2016).
- Groß, Hermann (2012): 'Polizeien in Deutschland'. [online] <http://www.bpb.de/-/politik/innenpolitik/innere-sicherheit/76660/polizeien-in-deutschland> (accessed on 09.03.2016)
- Khodyakov, D. (2007), Trust as a process: A three-dimensional approach, *Sociology*, 41, 115–132.
- Koops, E.J. (2010), The internet and its opportunities for cybercrime, in: Herzog-Evans, M. (ed.), *Transnational Criminology Manual*. Nijmegen: Wolf Legal Publishers, pp. 735–754.
- 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 & Yar (2016), Applying routine activity theory to cybercrime. A theoretical and empirical analysis. *Deviant Behavior*, 37: 263–280.
- Martin, J (2013), Lost on the Silk Road: Online drug distribution and the 'cryptomarket'
- Rieser, Marcel 2014: *Dyniamic Capability und organisationale Kompetenz: Im Kontext von Veränderung und Effizienz*. Wiesbaden: Springer Gabler.
- Schnell, Rainer/Hill, Paul B./Esser, Elke 2005: *Methoden der empirischen Sozialforschung – 7. Auflage*. München: Oldenbourg.

- Schnorr-Bäcker, Susanne 2006: Moderne Informations- und Kommunikationstechnologien in Deutschland – Entwicklung in Wirtschaft und Gesellschaft. In: Statistisches Bundesamt: Wirtschaft und Statistik 1/2006, S. 33 – 44. URL: https://www.destatis.de/DE/Publikationen-/Wirtschaft-Statistik/Informationsgesellschaft/Moderneinfokommunikation.pdf?__blob=publicationFile, zugegriffen am 14.03.2016.
- Wall, D.S. (2007), Cybercrime – The Transformation of Crime in the Information Age.

V. Concluding remarks from the three case studies

The project team

Our research explored how criminal groups involved in criminal activities on, via and against the internet operate in Germany, the Netherlands and Sweden 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 selected police files from the three participating countries. In total we analysed 44 cases, 15 Swedish, 18 German and 11 Dutch cases. 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, 3) cases of extortion to gain money or power, and 4) cases of data theft and copyright infringement.

The number of identified suspects involved in those cases ranges from two to several hundred and is highly dependent on both the case and the perspective of the law enforcement authority responsible for dealing with the case.

The age of the suspects varies highly, even within individual cases and within individual crime activities. In some cases the offenders were remarkably young. Cyber-OC seems to attract younger offenders more than traditional forms of organised crime do, in which young offenders are quite exceptional (Kleemans & De Poot 2008; Van Koppen et al. 2010).

Among the case files we analysed, we saw a variety of crimes and crime groups. On the one hand there were traditional crime groups engaging in cybercrime and using cyber expertise, common knowledge about the use of the internet or specific tools to perform their criminal activities more efficiently or in a more sophisticated way. On the other hand, there were 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 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.

For each individual country, the research questions formulated for this study were answered in the concluding section of the country study. The general conclusion deepens the understanding of the phenomenon of Cyber-OC by offering a synthesis of various aspects of the individual country conclusions as well as implications for future developments and law enforcement.

In this general conclusion, previously mentioned findings will be expanded on and described in conjunction with one another. We have structured this section under different themes in order to highlight the new possibilities that arise when organised crime occurs within or touches upon the cyber arena. This does not mean that traditional forms of organised crime activities do not occur in Cyber-OC. What it does mean is that, in addition to these traditional activities, new phenomena arise owing to the possibilities of the virtual world. We focus mainly on these aspects because they shape the way Cyber-OC unfolds and they require a new approach.

Theme 1: Organised crime groups entering cyberspace

Previous research has shown that organised crime groups seek new opportunities on the internet to obtain illegal profits. This ICT use transforms the nature of their crimes. Traditional organised crime groups can use ICT to enhance the impact of offences such as drug smuggling, human trafficking, extortion, fraud, the sale of counterfeit goods and illicit gambling. Thanks to ICT, organised crime groups can commit these offences on a larger scale. This ICT-induced enhancement is called the ‘cyber lift’.

The findings of this project show how this ‘cyber lift’ is established in practice. It also shows that ‘entering the internet’ and collaborating with skilled ICT specialists not only enhances the impact of traditional offences but also opens the way for organised crime groups to become involved in computer integrity crimes.

A general finding in all three countries is that organised crime groups that initially only committed traditional organised crime offences do not necessarily need to possess ICT knowledge themselves to obtain a ‘cyber lift’. The necessary ICT knowledge can easily be obtained via the internet in at least two ways: firstly, through purchasing particular services of ICT specialists on underground markets (Crime-as-a-Service) and, secondly, by resorting to ready-to-use cybercrime kits or instructions, which enable the groups to prepare and commit cybercrimes themselves. When the services of an ICT specialist are used, this collaboration between the group and the expert is in some cases a ‘one-time’ occurrence, and in others it happens on a regular basis, depending on the quality of the services provided. In the latter case the criminal cooperation leads to the establishment of an ongoing ‘professional’ relationship with particular experts, especially when their credibility and knowledge are highly appreciated by the group. We saw examples of cases in which the performance of these ICT specialists was so crucial to the group that they were awarded significant parts of the criminal earnings.

The ease with which ICT specialists can be found broadens the range of possible cybercrimes and lowers the threshold for committing computer integrity crimes for groups without special ICT expertise. Our findings show that, in practice, organised crime groups resort to both: purchasing Crime-as-a-Service as well as benefiting from the special IT knowledge of some of their members. Crime-as-a-Service can be seen as a new type of lucrative criminal activity, as one individual can specialise in selling his or her services to multiple criminal actors (individuals or groups).

Moreover, we saw examples of organised crime groups committing technically sophisticated computer integrity crimes, not only by using Crime-as-a-Service, but also without buying extra support. This means that the organised crime groups are flexible enough to adapt to the digital environment in such a way that they do not depend on external support from technically skilled experts.

Developments: The accessibility of special ICT services enables organised crime groups involved in traditional organised crime offences to keep pace with groups with technically skilled members. This means that all organised crime groups can ultimately engage in the different forms of cybercrime distinguished in this report – computer-assisted crime, computer integrity crime, content crime and cryptomarkets – either on their own or through the use of criminal services. As a consequence, organised crime groups entering cybercrime are not less sophisticated, less dangerous or less difficult to deal with than criminal actors specialised in cybercrime. Besides that, more and more crime groups could benefit from this open market by offering or making use of technically advanced criminal services.

Implications for law enforcement: For law enforcement agencies, this means that organised crime groups entering cybercrime as well as Crime-as-a-Service could lead to a rise in all forms of cybercrime as more actors become involved. Firstly, it is important that law enforcement agencies, when investigating cybercrime, keep in mind that networks or even organised crime groups might be behind the offences and not necessarily only individual offenders. Secondly, they need to keep in mind that when investigating traditional organised crime offences the groups involved may be dependent on ICT, thus effective countering should include digital experts and digital techniques, including digital forensics.

Theme 2: Structure and organisation

Although criminal networks engaging in cybercrime gain attention from scholars from different disciplines, much remains unknown about the organisational structures of the groups or networks committing Cyber-OC. Orga-

nised crime groups can be strictly organised, with clear internal hierarchies, distinctive roles and tasks, or they can have the form of more loosely organised, changeable, fluid networks carrying out criminal activities in different combinations and without any central control. Besides that, these networks can be locally organised or cooperate internationally.

Previous research shows that the internet provides an opportunity structure for decentralised, flexible networks of loosely organised offenders who collaborate and distribute work based on knowledge and skills (e.g. Koops 2010, Leukfeldt 2016). However, it remains unclear whether this new opportunity structure also influences the organisational structures of already existing, more traditional organised crime groups, or whether these groups would keep their original organisational form.

The findings of this project show that the organisational structure of crime groups committing cybercrime does not necessarily deviate from the structure of crime groups focusing on traditional forms of organised crime. The empirical material shows a range of organisational structures, as is the case in all forms of organised crime. However, depending on both the crime group involved (existing or new groups) and on the kind of crimes they commit (computer-assisted or computer integrity crimes), the opportunity structure of the internet seems to affect the structure of crime groups differently. For existing crime groups that use ICT to enhance the impact of their traditional crimes, this 'cyber lift' has more influence on the modus operandi of their crimes than on the organisational structure of the group. Traditional crime groups more or less keep their organisational patterns, and previously existing power structures seem to remain intact. However, new players entering this crime field seem to organise themselves differently. For these groups the new modus operandi is associated with new, less strictly organised and more network-like organisational forms, although this does not hold for all new groups. There are examples of 'new groups' with stricter hierarchies, specific roles and regular cooperation.

When it comes to computer integrity crimes, new players and the existing crime groups seem to be organised in a similar way: a small core group of offenders actually commit the crimes, either supported or not by a loosely organised sometimes very broad network of co-offenders, used to complete the criminal activities or to transport money or goods.

For both computer-assisted and computer integrity forms of Cyber-OC, the organisational structure can be loose and changeable. In many observed cases, people seem to work together on an occasional basis. The composition of the crime groups seems to be more determined by the skills of the people involved than by stable long-term social relationships between offenders,

which makes these crime groups very flexible. As said, this trend is less evident for groups with a longer history of organised crime.

Newcomers in this crime field either act as sub-contractors or establish a chain environment where one person or group links to another that links to another, etc. The internet facilitates the development of connections between people and groups who by themselves would not be able to commit the chain of acts necessary to commit these technically complex crimes. This collaboration between people with special expertise, criminal ideas and necessary contacts offers new criminal opportunities.

Developments: Forms of Cyber-OC manifest themselves in many ways, ranging from strong and stable groups with clear power relations and a division of tasks, to loosely structured chain interactions that do not emanate from one single point. This deserves our attention, as the chain pattern comprises a fundamental new structure of how technically complex forms of cybercrime can be committed – forms in which different people perform different activities, scattered in time and space. When structured like this, the responsibility for the execution of the crime seems to be distributed among several people, and relationships between people become less important. Whether this form of crime will predominate in the future cannot yet be foreseen.

Implications for law enforcement: As organised crime groups are involved in cybercrime, it seems to be important for law enforcement agencies to check if and how offenders involved in more complex forms of cybercrime are embedded into organised crime groups or into chains of cooperating offenders. Both the logistics of the crime and the relationships (hierarchies, chains of command) between the offenders involved in this crime should be investigated. If there is a lack of attention to these organisational structures, taking out only a single offender, even an enabler, would mean that the rest of the group continues to exist. At the same time, given the specific characteristics of the chain structure, law enforcement cannot afford to neglect the role of single offenders, especially in the case of enablers, as they can be crucial for the ‘success’ of other criminals and groups.

Theme 3: Trust

Previous research shows that trust is an important and pervasive concept in everyday life as well as in criminal interactions. Traditionally, in a stable group of criminals, trust is something that comes through long-term collaboration between people. Participating in a stable group requires a person to be loyal to the group. Trust of that kind ensures that the crimes and the identities of the group members remain hidden. However, in exchanges between cybercriminals this ‘bonding capital’ or ‘thick trust’ is not emphasised.

Rather their relationships are built on 'thin trust' (Khodyakov 2007): weak ties that provide unique access to resources and opportunities outside of their immediate social circles. According to the literature, reputation is one of the primary tools for maintaining trust in the cyber world. It is interesting to find out how thick trust, which seems to be an important characteristic for criminal groups, and thin trust, which is typical for virtual collaboration and collaboration with experts outside people's own circles, characterises the collaboration between people involved in Cyber-OC groups.

The findings of this project show that in some of the studied organised crime groups, traditional forms of bonding and loyalty-building mechanisms are present, such as personal relationships, collaboration with trusted family members and friends, permanent personal contact, extortion, threats and violence. In other crime groups, especially those cooperating as looser networks with 'project-based' collaboration, trust seems to play a different role. Partners are selected based on reputation and previous accomplishments. Furthermore, anonymity in cyberspace makes cooperation less risky and changes the way individuals participate in the criminal act. The project findings indicate that in the case of looser networks, where the offenders only know each other from an online context, 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. Compared to the more stable groups, it is clear that 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 not however mean that they would trust each other in the offline world. The anonymity of the internet seems to give subjects adequate protection. This anonymous form of collaboration also influences the way in which agreements can be forced through threats. Physical violence makes way for cyberattacks. In the studied cases, trust seems to be measured by the skills and reputation of an individual, where reputation not only refers to technical skills and the fulfilment of agreements, but also to the way in which authority and cooperative behaviour can be enforced.

Developments: The relative anonymity of online identities has shifted the meaning of trust. As this online anonymity is extending to different domains, it is expected that the meaning of trust for entering a joint criminal act will change the nature of the crime groups. Besides these new forms of trust-building, more traditional and robust forms of trust, as provided by family members and friends and through power relations, seem persistent as well, especially when criminal activities are performed in the offline world where shielding one's identity and activities is less easy to accomplish. In the online world new ways to develop, maintain and enforce power relations become visible.

Implications for law enforcement: These new forms of trust entail new challenges for the law enforcement authorities. The fact that skills can be more important than loyalty stimulates some crime groups to operate with 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. Therefore, prosecuting individuals' co-operating partners in this development by means of traditional law enforcement will prove to be more difficult. This is also true for more stable and hierarchical Cyber-OC groups, which often use sophisticated means of internal concealment, making it also difficult for law enforcement agencies to get the bigger picture and identify the different players working together to commit technically and sometimes also logistically complex crimes.

Theme 4: Cyberspace and cyber logistics

Previous research shows that organised crime operates both within and outside the logistic structures of the law-abiding community. Technological advances have always provided new logistic efficiencies and opportunities for law-abiding society as well as for criminal organisations. International supply chains and cross-border facilities have always been very beneficial to criminal groups. Cyberspace definitely enhances the possibilities to collaborate anonymously and on an international level, making the geographical position of actors of no or only minor importance. Traditional organised crime groups use existing logistic structures, such as marketing channels and community services, as well as self-established structures to be able to operate unnoticed, outside the law-abiding community. Cyberspace makes it easier to collaborate anonymously and unnoticed. The question is how the characteristics of cyberspace and ICT structures influence the degree to which Cyber-OC can be carried out within the law-abiding community or to what extent Cyber-OC requires new logistic structures.

The findings of this project show that crime groups that use the internet to enhance their more traditional forms of organised crime continue to use self-established structures in relation to marketing channels in order to conduct criminal activities. The studied networks and groups mainly use self-administered websites or online forums where illegal products can be sold and bought. However, they also use legal logistic structures, such as mail companies and legal financial structures.

However, when it comes to more technically advanced forms of computer integrity crime, the structural procedures differ. Criminal organisations and net-

works involved in these new crimes mainly use already established structures of law-abiding society and do not need to construct their own. Project findings show that crime groups involved in computer integrity crimes use infra-structures and databases of law-abiding society to gain access to the desired information or property of the victims. Hence, these organisations are not only operating within law-abiding society but are also dependent on the ICT structures of companies and authorities. In this way, organised crime has 'entered' the law-abiding cyber society.

Developments: As society continues the digitalisation process, more possibilities for organised crime groups are created. On the one hand, ICT opportunities allow rather inexperienced people without a global network to engage in organised crime offences on a global level; on the other hand, new ICT structures include a potential danger of crime since they facilitate ways of gaining access to new or higher criminal earnings.

Implications for law enforcement: As the development of ICT and corresponding cyber logistic structures continues, the pressure on law enforcement authorities to keep pace with these developments also increases. On the one hand, law enforcement agencies should try to recognise, understand and investigate these crimes, and anticipate both new forms of cybercrime and new criminal collaborations by understanding how technological developments create new criminal opportunities. On the other hand, it is important to strengthen the awareness of ICT developers regarding possible abuse of their systems and to increase their responsibility to develop security measures for crime prevention. In order to develop targeted security 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 digital systems and appropriately adapted built-in security and control mechanisms.

Theme 5: Initiation of crimes and crime groups

Previous research shows that crime groups involved in cybercrime can be relatively stable over time. In those crime groups, members know each other and share ideas for new crimes. These ideas are sometimes initiated within the group, in other cases some core members can be seen as initiators and coordinators, and may or may not communicate their ideas to trusted members involved in activities that need to be carried out to accomplish these initiatives. However, Cyber-OC networks can also consist of fluid chain-like structures, where information and goods seem to be more or less coincidentally exchanged between, or used by, different parts of the network. The question

is how the initiation of crimes and the formation of crime groups takes place within these sometimes loosely organised chain-like networks.

The findings of this project show a change in the initiation of crimes and the formation of crime groups as the internet further enables contact between people and offers new opportunities for splitting things up and outsourcing. Our data shows that the initiative for a crime sometimes comes from one or a few suspects who come up with an idea of how to make money in an illegal way. After the idea is born, the recruitment of people starts and can take place in an offline or online environment. Online recruitment is based on the expertise and skills individuals have and are willing to sell. People find each other on forums or websites where they promote their skills and can be hired for a job. Shared traits that connect people in the physical world, such as personality, social background, education and mother tongue, seem to be less important in cyberspace. The formation of the group is based on the skills and expertise required to commit the crime. In such cases the group structure is loose and highly dependent on the specific activities that need to be carried out in order to commit the crime. These loose and unstable groups conducting less tightly planned crimes are found alongside the more traditional collaboration between people built on social relations, such as friendship or family ties.

In many cases, accomplices and sub-contractors did not have the whole picture of the criminal set-up or were following the ‘no questions asked’ approach, in a way comparable to the fragmented organisation of modern production and distribution. One person can be the sub-contractor in one set-up and the perpetrator who commits the final offence in another. Roles are changing and services are purchased. The actual work accomplished by a single perpetrator is diminished and it is less clear who is responsible for the general criminal acts. However, the role of the internet, and the services carried out with the help of the internet, is increasing. The ‘machine’ seems to be becoming the hub of the wheel.

Developments: Ideas for crimes determine group formation, and groups in turn determine how crimes evolve. New technological developments and new ways of making contact with skilled co-offenders give rise to new crime opportunities. The initiation of crimes and the formation of crime groups will be organised and co-ordinated increasingly less with a top-down approach and more as the result of creative new partnerships and ideas that evolve from those new kinds of collaboration. Besides that, the perpetrators’ handicraft might increasingly be replaced by the ‘machine’, and the internet might come up with solutions concerning, for instance, sub-contractors and software.

Implications for law enforcement: With these new ICT-enabled working methods and ways of collaborating between suspects, it becomes more diffi-

cult for law enforcement to identify important actors or initiators within a criminal group. Actors change roles and can be involved in different groups, and group structures can change rapidly. When groups become more fluid, they are more difficult to identify, localise and get to grips with. This means that law enforcement agencies have to consider these groups within the context of their complex adaptive dynamics. This demands a broad scope and the long-term intervention effort of law enforcement agencies, since they have to focus on a dynamic, changing process rather than a fixed group with stable roles and activities.

A complementary angle could be to recognise that the perpetrators', sub-contractors' and facilitators' actual criminal act and their criminal intent have to some degree diminished as a consequence of this chain structure. Prosecuting single individuals in this development by means of traditional law enforcement strategies might be difficult. Instead, more attention should be directed to the 'machine', i. e. to incorporating security into the technical systems.

Theme 6: New windows of opportunity

Previous research shows that organised crime groups involved in cybercrime activities use the internet, amongst other things, to sell illegal goods or services, to deceive customers, to steal money from bank accounts or personal data from social networks, to blackmail individuals or companies. ICT can lead these groups or networks directly to the victims and it can also bring the victims – as buyers/customers – to the offenders, for example in cases of fraud where the victims themselves initiate contact with the offenders. ICT enormously facilitates the identification and damaging of victims – be it through mass spam emails or drive-by infections (where victimisation happens in an automatic manner, e.g. by being part of a botnet) or through specific attacks with the help of social engineering. Victims are quite vulnerable to cyberattacks. Just being online makes people vulnerable to cybercrimes such as malware and threats, while activities such as online buying increase the risk of online fraud, and being active on forums and social network sites increases the risk of hacking victimisation (Leukfeldt & Yar 2016).

The findings of this project show that there are indeed many new crime opportunities as a result of: 1) new contact areas between offenders and victims, 2) more sensitive information available on the internet – for instance in databases that are hacked and misused – and 3) companies using more and more computer-controlled procedures that are vulnerable to hacking and that change the way and the ease with which crimes can be committed without physical contact between the victim and offender. In addition, we also found a new dimension in terms of identifying and approaching vulnerable co-of-

fenders, who are often unaware of their active participation in a criminal group. ICT gives suspects new opportunities to get into contact with these co-offenders or 'supporters', who can play a crucial role in the observed criminal activities. Recruited supporters are often money or parcel mules, but they can also have other functions. As these vulnerable actors are mostly deceived by the offenders, they can also be seen as victims.

Developments: As our societies are undergoing a process of digitalisation at a tremendous pace, there will be further contact areas where suspects can access victims. There will also be more institutions with online databases containing sensitive information about their clients, which can be stolen and misused by cybercrime groups, and more companies with computer-controlled procedures that can be hacked or hijacked to attack others online. These developments cause Cyber-OC to incorporate a larger variation of crime types, where crime in a physical environment and cybercrime merge. This may lead to hybrids such as cyber terrorism, and acts of violence committed with ICT, for instance by hacking pacemakers, cars, homes or, on a bigger level, (nuclear) power plants.

Implications for law enforcement: Owing to the (physical) threat potential of Cyber-OC, it might be necessary to have a stronger prioritisation and to have a closer look at these new contact areas between offenders and victims and at new crime opportunities. One obvious implication is that preventive measures in general are even more important since the misuse of ICT can affect large parts of the population. One suitable approach is to put more effort into identifying vulnerable parts of society instead of only targeting potential suspects. At the same time it is important not to neglect the possibilities of new investigation measures. Combating crime is still very much a national matter and the police and other authorities are still more occupied with criminal activities on the street than with activities in cyberspace. Introducing new codes of criminal procedure, and new penal codes could be a solution to enlarge the possibilities to investigate and prosecute criminal acts in cyberspace.

Theme 7: Long-term activities

Previous research shows that complex criminal activities, which require preparation time and consist of different linked activities, performed by different subjects, do not necessarily fall under the title of organised crime. The term 'organised crime' refers to both the complexity of the crime and the long-term perspective of the groups or networks committing these crimes with their ability to conduct ongoing criminal activities. 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 less close contacts and fluid online relationships.

The findings of this project 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 new crime groups emerging in the cyber field, this long-term perspective takes on a different form. Although individuals seem to have this perspective, the groups or networks they are involved in to commit a particular crime do not always have 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. This seems to be less necessary as well, because trust between the people involved in criminal activities is less based on long-term cooperative relationships. The long-term perspective thus seems to become an individual’s choice or characteristic, and the groups are no longer dependent on the long-term commitment of their co-offenders.

Developments: Offenders involved in Cyber-OC are creating a new marketplace of subjects who can be hired for single specific occasions or for long-term involvement. The organised crime groups or networks operating in the cyber domain can use this marketplace either to recruit individuals with high technical knowledge or to buy their services. Hence, they can continuously develop their criminal activities and make them technically more advanced. For individuals involved in such changeable types of collaboration, the flexibility of the marketplace provides a structure where temporary organisations are formed and can be used for longer or shorter criminal set-ups.

Implications for law enforcement: The ability to rent out technical ICT knowledge increases the technical advancement of computer-assisted crimes. The marketplace enhances the features of single individuals, which makes organisational structures less stable and more resistant to external investigation and identification. In these cases, the success of an organisational approach, directed towards stable relationships and long-term activities, will decrease. Good insight into how the criminal activities of individuals are linked to other

activities and networks and insight into the role each subject plays in these changing networks will be necessary for a targeted approach to this phenomenon.

Theme 8: The term ‘organised crime’

Previous research shows that there has always been discussion concerning the term ‘organised crime’. Exactly which crimes or crime groups does this term cover? Traditionally the term is used to refer to serious and complex criminal offences such illicit trade, or trafficking in human beings – but it can also refer to crime groups and their organisational structure independent of the specific criminal activities they perform. Now that the internet is being used more and more to commit crime, or to facilitate crimes and crime groups, it is important to consider how these ICT-induced developments in the crimes and in the organisational structures of the crime groups influence our concept or the term ‘organised crime’.

The findings of this project show that the above-mentioned developments have brought about some new forms of crime that were not incorporated in the concept of organised crime before, and have brought about crime groups with new organisational structures that may not have been defined as criminal organisations before. These new forms of crime and ‘criminal organisations’ arise alongside more traditional crimes and organisational structures in the cybercrime domain. We will focus on these new forms because they affect our thinking about existing concepts.

The studied Cyber-OC groups have different organisational structures, ranging from strictly organised groups to loosely organised networks. Within these loose networks the cooperation between suspects often takes the form of a chain linking people involved in different activities that together constitute the criminal act. These chain structures have different characteristics that are relevant when it comes to deliberations on the concept of organised crime, namely:

- Suspects getting involved in organised crime without knowing it. This aspect is not new or striking for organised crime groups. There have always been suspects involved in organised crime cases that were part of a crime group without knowing it. For security reasons, strictly organised crime groups often shield different activities or different parts of a group or network from each other.

- Within this chain structure, suspects are working together, being responsible for a single part, but together shaping the crime as a whole. To express it more visually: each suspect is one piece of a puzzle; the puzzle does not exist without the pieces and the value of the pieces cannot be assessed without taking account of the complex puzzle. In organised crime, this is not new either. In more strictly organised crime groups, tasks are also often divided, meaning that each suspect is responsible for specific parts of a coherent plan of activities as well. This can be achieved within different organisational structures.
- Suspects do not need to have knowledge of the entire criminal act they are involved in, they do not have to agree on the general plan, and they do not have to consciously work together to contribute to the realisation of this plan. These characteristics are not new either and are actually quite typical of certain subjects involved in organised crime. In traditional organised crime groups, so-called facilitators quite often commit essential and necessary criminal acts that meet this characteristic of ignorance.
- Suspects can work together and depend on each other without knowing who those others are. In itself, this aspect is not new either. In the offline world it also happens that suspects involved in a specific criminal organisation depend on each other without knowing who the co-offenders they depend on are. However in those cases there is mostly an intermediary who coordinates these different activities and ensures confidence by controlling these different suspects. Owing to the internet, this coordinating of activities can now be done without an intermediary being aware of the specific activities and of the ultimate goal.
- No one has to be in control, there is a fragmentation of the criminal act and often there is even 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 has 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 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 from the bottom up, rather than being organised in a top-down way. This way, crimes as well as crime groups seem to more or less co-incidentally arise and take on a certain form.

Developments: The crucial role ICT is already playing as a tool for the commission of traditional crime is going to gain more and more importance. Computer integrity crime 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, where people are buying and selling stolen data from anonymous sellers while no one really knows where the data is coming from and what is really happening with it in the end. As a consequence, there is huge diversity and uncertainty, and it is difficult to allocate crimes to specific crime groups or criminal organisations and to predict how crimes will take shape.

Implications for law enforcement: On the one hand, law enforcement agencies should incorporate IT experts into investigations of serious and organised crimes, as ICT can pervade all steps of a crime. On the other hand, existent ‘traditional’ measures will not be enough to successfully investigate organised computer integrity crimes because, besides the already known organisational structures, new structures and new forms of crime have emerged that require appropriately adapted concepts and tactics, focusing on ‘enablers’, where you see the subject’s responsibility for their own actions and for the way they enable others to commit crimes. Although it will be difficult to find out whether a perpetrator is acting in a coordinated manner, the acts in themselves can be addressed.

Final remark

All in all, technological developments will further expand the possibilities to interact anonymously. Cybercriminals, evidence, profits and victims will 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 laws seem to be necessary.

In the Netherlands, the Minister of Security and Justice recently made a proposal to give Dutch law enforcement the authority to hack devices of criminals in the hope of getting hold of information that would otherwise be out of reach for the police. In Germany, the Minister of Justice of the State of

Hesse suggested the introduction of a law that penalises the infection of computers with malware that makes the affected computers part of a botnet.¹²⁹

New local and international laws are 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 joint report, written by researchers of three European countries, has contributed to this goal.

¹²⁹ <http://www.spiegel.de/spiegel/vorab/initiative-gegen-botnetze-a-1081856-druck.html>, (accessed 12. 03. 2016).

VI. Appendix – Literature review

Dorothee Dietrich, Karsten Kasper, Gergana Bulanova-Hristova

Contents

- 1 Introduction 241
- 2 The internet and the perpetration of crime 243
- 3 Myths about cybercrime 245
 - 3.1 The myth of offender characteristics 245
 - 3.2 The myth of ‘always’ international characteristics 246
 - 3.3 The myth of hierarchical structures 246
- 4 Structural characteristics of cybercrime 248
 - 4.1 Typology of cybercrime 248
 - 4.2 Cybercriminals¹³⁰ 251
- 5 Organisational structures 256
 - 5.1 Lone operators versus organised groups 256
 - 5.2 The heterogeneity of organisational structures in cybercrime 260
 - 5.3 Typology of cybercrime groups 271
 - 5.4 Size of cybercrime groups 273
- 6 Involvement of organised crime in cybercrime 274
- 7 Conclusion 280
- 8 References 281

Figures and Tables

- Figure 1: Different levels within underground marketplaces 266
- Figure 2: The hierarchy of the ‘Digital Mafia’ 270
- Figure 3: Traditional mafia structure 271
- Table 1: Typology of cybercrime groups 272

¹³⁰ For a detailed elaboration of different typologies of hackers: Bundeskriminalamt 2015: *Täter im Bereich Cybercrime – Eine Literaturanalyse*.

1 Introduction

Worldwide the digitalisation of society is proceeding rapidly and influences almost all areas of life. The growing integration of the internet also provides new opportunities for criminal activities. In academic literature there is increasing evidence that ‘traditional’ OC groups are also progressively benefiting from this development, committing more and more crimes on, through and against the internet and information and communication technologies (Broadhurst et al. 2013: 19). It is not only the involvement of organised crime in cybercrime that has been found to be dangerous, but also the evolution of well-organised cybercrime groups, which are partly characterised by their own so-called ‘cyberborn’,¹³¹ structures. The special feature of this is that they have their roots in cyberspace and that they proceed in an organised and collaborative manner. Therefore, the fight against Cyber-OC – i. e. against off-line criminal groups that commit cybercrime, on the one hand, and against cybercrime groups proceeding collaboratively on the other hand – presents a particular challenge for law enforcement agencies. This means, among other things, that the strategies for combating crime have to keep up with this development (Schönborn 2013: 34).

The international EU-funded project ‘Cyber-OC – Scope and manifestations in selected EU member states’ aims to shed light on the links between cybercrime and organised crime in the three participating countries and on how these two phenomena impact on each other. In the course of the project the three participating organisations, the German Federal Criminal Police Office (BKA), the Swedish National Council for Crime Prevention (Brå), and the Dutch Research and Documentation Centre (WODC), each carried out a national empirical case study. The literature review aims to systematically process the state of research in the field of Cyber-OC on the basis of open sources.

In this process, the following questions formed the primary focus:

- Which topic-related definitions can be found in academic literature?
- How do OC groups use the internet to commit ‘conventional crimes’?
- What type of cybercrimes do they commit?

¹³¹ A term developed during the project to describe structures or groups that have emerged from a cyber environment.

- To what extent does the internet affect the structure of OC?
- How do ‘cybercriminals’ cooperate and is cybercrime organised?

Sources that dealt with the overlap of organised crime and cybercrime as a matter of priority were evaluated. The first step included a systematic, keyword-based search in order to identify research projects, studies, doctoral and diploma theses, professional articles, convention work and monographies in English, German, Dutch and Swedish relevant for the review. Previously determined search terms were used to search online (including in library catalogues and on the websites of relevant institutions) as well as through specific databases containing relevant literature.¹³² In addition to the keyword search, literature was also searched for using a ‘snowball system’, which means that further articles were identified through the bibliographies of particularly relevant literature.

These focus on cybercrime that is committed by various suspects in a work-sharing manner, and/or on criminal groups that committed offences with the help of ICT or offences against ICT. Based on this, the following criteria of relevance for the content-related categorisation were determined: no reference, indirect reference and direct reference. This content-related verification was done with the aim of evaluating solely relevant publications.

The literature search performed by the three project partners resulted in a great number of matches, of which the majority was written in English. After the first screening of research results, it was recognised that the majority of sources either focused solely on organised crime or on cybercrime. As such sources do not illuminate the interdependence of the phenomena to a sufficient extent, they were not taken into account for the review. In addition it was shown that the intersecting set of OC and cybercrime was primarily found in theoretical literature and has rarely been the focus of empirical investigations. In total 140 publications, published between 1997 and 2015, were identified. The contents were systematically summarised with a coding system regarding the research question in the period from the end of 2014 to the beginning of 2015.

The phenomena Cyber-OC can be exemplified in two ways based on the working definition: on the one hand it can be analysed as the way cybercriminals cooperate: this includes for example the question as to the cooperative structures and practices that have been developed in this relatively young field of phenomena. On the other hand, the concept of Cyber-OC also in-

¹³² Such as by searching for the terms ‘Cybercrime / Internet crime and organised crime’ in English, German, Dutch and Swedish.

cludes criminal groups that use ICT to simplify the perpetration of a crime or that discovered cybercrime as a new main field of activity and additional source of income.

The impact of the internet on the perpetration of crime according to the academic literature will be illustrated further in chapter 2. In chapter 3 various widespread assumptions about cybercrime will be dealt with. While chapter 4 refers to the different forms of organisation in cybercrime, chapter 5 focuses on questions concerning the participation of traditional criminal (OC) groups in cybercrime, as well as on the impact of ICT on their procedures.

2 The internet and the perpetration of crime

One of the main aspects of the scientific approaches to the phenomena of cybercrime and Cyber-OC concerns the effects of ICT, and particularly the internet, on the perpetration of crime. The statement that the internet leads to a 'deterritorialisation' (Koops 2010: 740) meets the consensus; this term means that offences that are committed on and through the internet are international phenomena that present additional requirements for the strategies of law enforcement. Moreover, there is also a consensus regarding the assumption of growing global networking through the internet and that it presents unprecedented possibilities for criminal offences. This includes both the choice of victims and the procedure of perpetrators, their communication with each other, as well as the creation of markets for illegally obtained assets. Furthermore, information gathering, communication and logistics for the perpetration of 'traditional' crimes in the non-virtual space are facilitated through the use of computer technology.

The low cost and time efficiency are seen as the greatest advantages for perpetrators of internet-based offences. Accordingly, cybercrime is considered to be very lucrative for offenders, since it generally requires little infrastructure and little personnel deployment. Software or the lacking know-how can be bought directly from experts through online trade forums. Personnel placement can, unlike criminality in the non-virtual space, be reduced to a minimum despite the international reach that can be achieved through internet-based offences. Communication and networking are facilitated for criminal groups as well as for criminals acting alone as the internet allows symmetric and asymmetric social relations, in other words, information can be transferred between individual criminals and criminal groups and vice versa through encrypted communication channels. By this means, new members can be recruited and trained. Moreover, the organisation and coordination among them can be accelerated.

In connection with the meaning of the internet for the perpetration of crime, the possibility of power and the range of individual perpetrators are also discussed in academic literature. Attacks by means of the internet can be committed repeatedly, in real time and from almost anywhere in the world by automated means with a great damage potential for many victims simultaneously. Thus according to Wall (Wall 2014: 229) the crime is being 'democratised' because it allows perpetrators to commit a crime that was previously beyond their financial and organisational means and that was only feasible for 'traditional' OC in the described scope (Lavorgna 2014: 265).

Additionally, cybercrime not only features financial damage but also causes citizens' loss of trust in computer systems and harms the credibility of digital transfers and the free market:

'[...] phishers trick users into handing over cash, credit-card data, social security numbers and endless amounts of other valuable information. [...] Phishers are hurting more than the user – they're punching a Mack truck-sized hole in user confidence [...] industry leaders say.' (McCafferty 2004)

'But the damage here goes far beyond hosts. It takes away from the universal promise of the Internet, really – the promise that it has to reduce costs and provide an interactive experience with customers online. It damages the whole credibility of the email transaction. And that puts a damper on e-commerce in general, which ultimately hurts hosts and everyone else with a stake in it.' (McCafferty 2004)

In literature, the low risk of discovery for the offenders is seen as another great 'advantage' for perpetrators of cybercrime. The segregation of 'real' and 'virtual' identity as well as the international perpetration – various judicial systems are affected and the responsibilities are often not clear – complicates detection and prosecution. The anonymity that is attributed to perpetrators on the internet with regard to the police and competing criminals is not solely seen as an advantage for the criminals, according to Lusthaus. He assumes that this also represents a challenge to establish and maintain trust between cybercriminals for the cooperation of various cybercriminals or for sanctioning unreliable group members (Lusthaus 2012: 71).

Because of the internet, the amount of offences, as well as their scope, is increasing. Owing to the exploitation of new distribution channels, for instance through social engineering within social media, the participation of different types of criminals in cybercrime is favoured: the range of pharmaceutical crime can vary from an individual criminal, through a small group of cybercriminals, up to big networks or 'traditional' OC. The threat level equally varies from small nuisances to great financial losses for individuals, firms or states. Here the internet can convey the impression to the criminal that the act is not real, as it is committed from a distance and no direct contact with the

victim is made (the Swedish National Council for Crime Prevention 2000: 14).

The work of law enforcement agencies finds itself faced with new challenges: contrary to the perpetration of crime in the non-virtual space, cybercrime is characterised by fast changes in crime opportunities and procedures owing to technological innovation. The commission of a crime through the internet further allows many small attacks on a variety of victims, which, viewed individually, represent very small damage, and are often not reported by the victims and therefore not prosecuted. However, taking into account the total incurred financial costs that are achieved by the means of these ‘salami techniques’ (Koops 2010: 740) (also called ‘micro-fraud’, Wall, 2010b: 60), their meaning and threat becomes visible.

3 Myths about cybercrime

Often in media reports and literature one can find widespread assumptions in relation to cybercriminals and (organised) cybercrime, which frequently are not based on empirical evidence.

3.1 The myth of offender characteristics

One of these assumptions is that the typical cybercriminal is young, technologically gifted, socially awkward, and that he suffers from some kind of mental disorder.

‘One of the myths challenged throughout the course of my fieldwork was that cybercriminals are all young, socially awkward and sometimes suffering from various mental disorders and disabilities.’ (Lusthaus 2012: 77)

Even though there are several cybercriminals that are directly attributable to this group, Lusthaus emphasises that in fact a variety of different perpetrators are involved in cybercrime (see *ibid.*). The Detica/BAE Systems study refers to the inaccuracy of assumptions in relation to the technological skills and the age of cybercriminals.

‘The popular image of the “cyber criminal” – the youthful “computer geek” scheming remotely in his bedroom [...] Contrary to what one might anticipate, digitally-enabled crime goes far beyond hacking, and our assumptions about the youth and skill level of digital criminals are skewed.’ (Detica/BAE Systems 2012)

Correspondingly cybercriminals do not always have, as often assumed, extensive knowledge of technology, as a major part of the necessary infrastructure

and tools can be purchased online without the need for special computer literacy (Detica/BAE Systems 2012). This development is also described by the United Nations Office on Drugs and Crime (UNODC):

‘Cybercrime perpetrators no longer require complex skills or techniques, due to the advent and ready availability of malware toolkits.’ (UNODC 2013: 39)

Moreover, the assumption that cybercriminals are mainly hackers acting alone who barely have social contacts and instead spend the night-time on their computers cannot be confirmed. Instead, the literature indicates that there is more than ever to steal online, which causes professionals and well-networked criminals to increasingly enter cybercrime (McCafferty 2004).

‘The image of the hacker or Internet scammer as lonely, dateless loser pecking away at the basement computer by night no longer applies. The stakes are higher now. There is more than ever online to steal.’ (ibid.)

3.2 The myth of ‘always’ international characteristics

As ICT favours an international perpetration of crime, it is often assumed that cybercrime is always committed in an international context and that cybercriminals barely know each other in real life. However, the above-cited study acknowledges that many cybercrime groups are influenced by local contacts and circumstances. According to the study, regional and national features have an impact on group structures, therefore it is not unusual that even local criminal groups join forces to commit cybercrimes (see *ibid.*). This statement is supported by UNODC, which asserts that cybercriminals recognise and make usage of the geographical, cultural and linguistic proximity of trust-building elements (UNODC 2013: 49).

3.3 The myth of hierarchical structures

In addition, the assumption that the structures and organisational forms of cybercrime groups are always geared to the traditional, hierarchical structured (mafia) model of organised crime is not empirically confirmed (Wall 2014: 228). Wall suspects, for instance, that the myth of mafia-like organised cybercriminals is based on an everyday logic, which assumes that the rapidly growing threat and the damage of cybercrime are only possible through the connection of cybercriminals within mafia-like structures. This simplified image of mutual interdependencies between OC and the internet is strengthened by the fact that several servers used for cybercrime are located in Russia and Eastern Europe, thus in countries where traditional OC is widespread and where many OC groups originate from. Wall assumes that cybercrime is com-

mitted through an organised form, but instead of adopting mafia-type structures, perpetrators adapt their group structure to the new crime opportunities of the internet and therefore are not comparable with traditional OC; he refers to the prevalent geographical dispersion of criminal groups and their relatively flat hierarchy (Wall 2014: 237). Even McCusker emphasises that cybercrime is often described as organised, which does not necessarily mean that members of OC groups are actually involved (McCusker 2006: 2).

‘Equally, it seems common to refer to cybercriminal “groups” as if they were of equivalent size, complexity, “stature” and duration as their traditional, non-virtual counterparts. This effectively allows cybercriminal groups to achieve the semblance of the organisational evolution actually achieved by those traditional organised crime groups they are deemed to emulate.’ (ibid.)

Since cybercriminals, without having comprehensive organised structures, are often equated with OC, and no distinction is made between the complexity and gravity of a crime, the myth about cybercrime, for example in relation to its distribution, gravity and opaqueness, is nurtured and maintained (ibid.). Thus it remains uncertain for McCusker whether traditional OC groups are actively participating in cyberspace (McCusker 2011: 116). It is estimated that these traditional OC groups do not have the necessary and sufficient expertise to commit cybercrime and that they are depending on organisational and geographical proximity as well as on the use of violence.

Nonetheless the Detica/BAE Systems study, for instance, notices that long-established, traditional OC groups are in fact shifting their activities more and more into a digital context (Detica/BAE Systems 2012). On this note, another source clearly shows that at least two out of the five strictly hierarchically structured families of the Cosa Nostra in New York are involved in cybercrime. Correspondingly, members of the Gambino ‘family’ are suspected of being part of widespread online fraud, which is stated in the following sources:

‘According to reports, US prosecutors made several indictments last month against Lexitrans Inc. and other shell companies based in Overland, Kansas, alleging that they ran adult Web sites and 900 numbers, defrauding customers by illegally charging for subscriptions to services that were advertised as free. Lexitrans is alleged to have been founded by members and associates of the Gambino crime family. According to reports, the scams ran by Lexitrans netted around \$230 million for the perpetrators.’ (The WHIR 2004)

‘According to published reports, this was no basement-level operation. There was no less than 7,000 square feet of data center space at the Overland Park location, with redundant power and fiber-optic pipes. Internet access costs were estimated at \$50,000 a month, and the company was paying \$100,000 every day for placement on popular search engines.’ (McCafferty 2004)

On the other hand, offenders with connections to the Bonanno ‘family’ were sentenced for data theft and blackmailing.

‘Lexis-Nexis made public notification of a data breach that federal authorities say is tied to a New York mafia crime family. The New York-based company has sent more than 13,000 letters to former customers whose personal data may be at risk. The 13,000 customers may have been targeted for extortion and identity theft. Earlier in May, the U.S. Attorney General’s office in Southern District of Florida handed down an indictment charging 11 men with racketeering conspiracy. The 11 had ties to the Bonnano [sic] organised crime family.’ (McGlasson 2009)

The authors of the Detica/BAE Systems study assume that cybercrime gives rise to new criminal actors. Similarly dangerous are the new possibilities, referring to the extension and improvement of activities that cybercrime brings to those traditional organised crime groups entering cyberspace.

4 Structural characteristics of cybercrime

To better understand the varying motives and types of *modus operandi* of the perpetrators, a comprehensive examination of the complex phenomena of cybercrime and its overlap with OC is needed. Whereas the research on cybercrime is advanced, there are, as yet, only a few statements about the personality of perpetrators¹³³ or cybercrime groups.¹³⁴ In this chapter the different approaches to cybercrime and cybercriminals and their forms of organisation are dealt with. In order to allow a comparison between cybercrime groups and traditional OC, already existing findings on the age structure of offenders and the size of cybercrime groups¹³⁵ are addressed.

4.1 Typology of cybercrime

4.1.1 According to historical emergence

Based on the stages of development of cybercrime during the past few decades, Wall differentiates between the following cybercrime ‘generations’ (Wall 2007: 44 et seq.):

¹³³ See, for example, Lusthaus 2013a.

¹³⁴ See, for example, Choo & Grabosky 2014.

¹³⁵ The terms ‘cybercrime groups’ and ‘cybercrime networks/collaborations’ are used synonymously.

First generation: This generation acts within discrete computing systems, using computers to assist traditional offending. The so-called 'low end cyber-crimes' include mainly criminal exploitation of mainframe computers and their discrete operating systems. Furthermore, computers are used as ICT during the preparation phase of a crime, though these crimes could have been committed without using these technologies.

Second generation: Cybercrimes belonging to the second generation gives opportunities for crimes across a global span of networks, such as hacking, cracking and the diffusion of illegal pornographic material. It combines knowledge of telephone systems, computing and social engineering to obtain information. Available personal computers, starting in the 1970s/80s, and the internet in the 1990s opened new possibilities in a global context. Still, the criminal ideas and crimes themselves remain traditional, therefore they are defined as 'hybrid' crimes. This can lead to criminal law issues; however, responsibilities, law enforcement and offences are still quite clear in this regard.

Third generation: This generation features a strongly distributed and automated element. The 21st century and the development of networked technologies and the possibilities that go with social engineering have led to a fearless perpetration of crime. These crimes represent the 'true cybercrime', which evolves solely through the internet and could not be committed without the use of technology. Offences fall outside the common jurisdiction and previous experience of law enforcement processes. Nevertheless, previous offences, such as hacking, should not be underestimated, as they will continue to be committed.

In literature it is discussed whether another fourth generation of cybercrime can be understood to have developed in compliance with Wall's categorisation. This means crimes that are exclusively committed in cyberspace and do not cause direct damage in real life. Conceivable are for instance the theft of virtual goods within an online role play or the abuse of avatars. However, this assumption is relativized by the fact that the crimes mentioned solely represent cybercrimes of the second generation, which are transferred completely into the virtual world. Additionally, it is questionable if these actions represent crimes at all as no concrete real victims are liable to suffer damage (Koops 2010: 3). Wall views the establishment of 'ambient intelligent networks' as a potential further stage of development of cybercrime given that the growing usage of ICT in everyday life (for example computer chips in clothing and buildings) and the constant interlinking of all systems represent additional crime opportunities for criminals (Wall 2010a: 98).

4.1.2 According to the use of information and communication technology

Besides the categorisation of cybercrime based on its historical development, a differentiation of cybercrime according to aims and procedures can be found in the literature. Accordingly, already in 1997 cyber offences were separated into three categories.

These firstly address crimes whose targets are computers or computer networks, for instance for sabotage purposes or to steal intellectual property.

The second category includes crimes where a computer is used for the commission of a crime, for example for making manipulated data or for the distribution of child pornographic material.

The third category covers offences where computers have been used circumstantially for the preparation or perpetration of a crime in one way or another. Here the usage of technology is not necessary for the perpetration of the crime, however it facilitates the process. Drafting a threatening letter can be named as an example (Goodman 1997: 469).

4.1.3 According to the function of the internet

While the above-mentioned typology made its differentiation based on the application of computer technology, the following differentiation addresses the primary use of the internet. This typology is used in the project's own working definition of Cyber-OC, and differentiates between the internet as a target, the internet as a tool and the internet as a space for the perpetration of crime.¹³⁶

1. Computer integrity crimes – crimes that are directed against the confidentiality, integrity and availability of computer data and systems¹³⁷ (for instance intercepting or interfering with data through hacking or the dissemination of computer viruses, or threatening by means of DDoS attacks): these offences target the safe access to computers or networks and are therefore only possible because of the usage of ICT. They can be used as a preparation for computer-assisted crimes, such as phishing. The internet is the target for the perpetration of the crime.

¹³⁶ See Council of Europe 2001; Koops 2010: 2; McGuire & Dowling 2013: 5; Wall 2010a: 99; Wall 2014: 228.

¹³⁷ Also referred to as cybercrime in a narrow sense.

2. Computer-assisted crimes – crimes by means of ICT¹³⁸ (for example counterfeiting, fraud, theft of identity): for this purpose networked computers are used in order to obtain money, objects or services. In other words they are ‘traditional crimes’ that are transferred into the digital space and facilitated by the use of ICT. The crime would have been possible without the usage of ICT, but only to a lesser extent. In this case the internet is used as a tool for the perpetration of crimes.
3. Computer content crimes – content-related crimes and copyright infringement (for instance distribution of child pornography or hate speeches, offences with the help of social networks): such crimes aim at the illicit content of networked computer systems and their distribution. The internet is used as the space for perpetration.

This last typology of computer crime into these categories represents an ideal typology, with the help of which the phenomenon can be analysed in a more structured way. The aim is to differentiate between various manners of perpetration or possibilities of enforcement. Phenomena such as phishing cannot be allocated unequivocally to one category, since they contain elements of several categories. According to Wall, however, there is often a visible main motivation behind specific offences (Wall 2010a: 99).

4.2 Cybercriminals¹³⁹

The literature argues that the phenomenon cannot be referred to as ‘the cyber-crime’, since there is no uniform criminal offence. Likewise, there is no such thing as ‘the cybercriminal’. A differentiated view shows that individual perpetrators differ with regard to characteristics, motivation and procedure and that there is no predominant ‘type of perpetrator’.

‘Cybercrime is no longer a ‘middle class’ crime of well-educated and privileged adolescents. As Internet access and usage has become more widespread, there are now cybercriminals from all backgrounds and demographics [...]’ (Lusthaus 2013a: 55)

The idea that cybercriminals are solely (young) hackers with good computer literacy might have been valid for the beginnings of cybercrime; meanwhile, however, IT skills can mostly be seen independently from the offender’s age. Owing to the establishment of the division of labour in cybercrime, individual

¹³⁸ Also referred to as cybercrime in a broad sense.

¹³⁹ For a detailed elaboration of different typologies of hackers: Bundeskriminalamt 2015: Täter im Bereich Cybercrime – Eine Literaturanalyse.

persons specialise in specific subsections while additional skills or tools needed are provided by other parties. Owing to this cooperation it is even possible to commit cybercrime without any form of technological understanding.

4.2.1 Findings about the age, gender and level of education of cybercriminals

Only a few empirical studies have focused on the age structure of cybercriminals. Alongside the lack of thorough discussion on the methodological approach, only very few assumptions can be made regarding the findings and their quality.

As already stated, at the beginning of the 21st century there had been a widespread assumption among scholars that cybercrime was carried out by young, talented, mainly male individuals. This view was shared by Europol, which described cybercriminals as '[...] young, highly skilled individuals who are often recruited from universities' (Europol 2011: 6) and who have the necessary expertise. Further on, Europol also emphasised that owing to the supply of cybercrime tools, it is also possible that even children and teenagers are involved. The authors quote a study by Chiesa, Ducci and Ciappi published in 2009, according to which 60 per cent of hackers from a sample at the date of the evaluation were under 25 years old and furthermore a proportion of 60 per cent of the investigated persons had already started with hacking between the ages of 10 and 15¹⁴⁰ (Chiesa, Ducci & Ciappi 2009, cited in Europol 2011: 6). Thus cybercrime in its demographic structure is similar to conventional crime as the quote below explains (UNODC 2013: 39 and Li 2008: 129).

'A noteworthy phenomenon is that whether it be individual cybercrime, corporate cybercrime, or organized cybercrime, young perpetrators play a critical part. Although there is no age limit to commit cybercrime, we found that, similar to traditional crimes, youth constitute an important proportion of the cybercriminals.' (Li 2008: 129)

'The demographic nature of [cybercrime] offenders mirrors conventional crime in that young males are the majority, although the age profile is increasingly showing older (male) individuals, particularly concerning child pornography offences.' (UNODC 2013: 39)

However, a study by Hutchings in 2014 indicates that the model of the young hacker does not apply anymore. The age range of seven active and former

¹⁴⁰ Accessed data: approx. 1400 questionnaires ('self-report questionnaires') filled in by hackers.

Australian cybercriminals who were interviewed by the author was between 18 and 49 years. Nevertheless, each one of these perpetrators had already entered cybercrime at the ages of 11 to 25 and therefore started at a similar age to the test persons of Chiesa, Ducci & Ciappi.

The analysis by Detica/BAE Systems leads to a similar conclusion. Out of 101 investigated offenders, 43 per cent were aged above 35. The proportion of 14 to 18-year-olds of the 101 perpetrators was even below the proportion of 50-year-olds (Detica/BAE Systems 2012). In accordance with these results, cybercrime could be a crime field which allows an early entry and a long-lasting career for criminals at the same time. However, meaningful empirical studies are yet to be made.

In relation to the perpetrator's gender, many studies conclude that an overwhelming majority of cybercriminals are male¹⁴¹ and moreover that the proportion of men within this phenomenon is significantly higher than in other fields of crime.

'Cybercrime perpetrators are overwhelmingly male [...]. Findings of more than 90 per cent correspond to a higher proportion of male involvement in cybercrime than for crime in general. Globally, the proportion of males prosecuted for any crime is typically between 85 and 90 per cent [...].' (UNODC 2013: 42)

Furthermore, cybercriminals hold, on average, a higher education degree in comparison to 'conventional' criminals:

'[...] education levels amongst cybercrime perpetrators may still be higher than for conventional, or all, crime. The Lu study [Lu et al. 2006] found 28 per cent of cybercrime suspects in the territory had undertaken tertiary education, compared with eight per cent for all crime. Similarly, the HPP study [UNICRI/Chiesa 2009] found that more than half of hackers had undertaken tertiary education. Nonetheless, as noted by the BAE Detica study, it is likely that the "artificial" acquisition of technical skills (such as through malware toolkits including ZeuS or the Butterfly Bot) has resulted in a shift away from the traditional profile of a highly-skilled digital criminal, towards a much wider pool of individuals.' (UNODC 2013: 43)

There are only a few analyses that deal with the question of cybercriminals' sentences. One of those is the study by Marcum et al., in which it is shown that people who commit cybercrime are sentenced comparatively rarely and, if it comes to a conviction, the sentences were relatively short (Marcum et al. 2012: 35 et seq.).

¹⁴¹ Between 81 per cent (Lu et al. 2006: 13) and 98 per cent (Li 2008: 132).

‘Relatively little is known about the sentences imposed on offenders convicted of cyber (or any computer-related) offenses. Information from the United States Department of Justice (2010) does show that for the five-year period of 2006–2010, a total of 1177 individuals were convicted and sentenced for cybercrimes. Of these, only 51.7 per cent (n=608) received a sentence including any prison time. For those who were sentenced to incarceration, sentences were typically fairly short. [...] In contrast to other types of offenses, this data suggests that cyber offenders may be among the least likely variety of felons to be sentenced to incarceration.’ (Marcum et al. 2012: 35 et seq.)

4.2.2 Motivation of perpetrators

Also the motivation to commit cybercrime has rarely been the focal point of empirical evaluations. Of course, some exceptions exist, for example in relation to specific crime types, such as cyberstalking and child pornography. The following illustrated arguments are therefore based rather on theoretical assumptions and results of literature analyses than on empirical outcomes. Furthermore, it is understood that the motivation for cybercrime has an effect on the decision as to whether a criminal commits cybercrime individually or within the framework of a group.

The Bundesamt für Sicherheit in der Informationstechnik (Federal Office for Information Security, abbreviated as BSI) identifies several offender types within cybercrime: cybercriminals,¹⁴² intelligence service, hacktivists / cyber activists, and internal offenders, each with a different underlying motivation. Here, the main motivation of cybercriminals is financial enrichment. Their focus lies on data, services or online accounts of individuals or companies, which are subjected to extortion, deceived or spied on for competitors. Organised cybercriminals mostly act highly professionally, in contrast to individual offenders or small groups. The procedure of cybercriminals is dependent on the technological progress and the existing defensive measures. As long as cybercrimes are financially worthwhile and the cost-benefit calculation produces a positive result in terms of the rational-choice approach, they will be carried out. According to the division by the BSI, intelligence services commit cybercrime mainly for espionage purposes. By means of Trojans, economic espionage is conducted for a state’s own purposes or to strengthen the national economy. Intelligence services have the best resources for cybercrime within the varying offender types and are only limited through their own application of those resources. In comparison to most cybercriminals,

¹⁴² The term ‘cybercriminals’, in this paragraph, is merely used as a possible model of multiple models of perpetrators. In the remaining report, the term solely refers to criminals in general who commit cybercrime in a narrower and broader sense.

they proceed much more professionally and also use particularly developed malware besides the available standard tools on the internet (BSI 2014: 23 et seq.). The main motivation of hacktivists or cyber activists is, according to the BSI, public protest against an experienced deplorable social, economic or technical situation. Even though 'solely' a purely ideological goal is pursued, states, state organisations or commercial enterprises are sometimes harmed massively. Simultaneously to attacks in the digital world, whose range covers everything from the manipulation of websites for the purpose of disinformation through to data theft and its publication, protests are performed in the real world as well. Besides various groups, individual perpetrators also act and organise themselves rapidly when needed (BSI 2014: 23 et seq.).

Based on the motivation of perpetrators, Lusthaus, too, differentiates between various types of cybercriminals, which are partially congruent with the offender types named by the BSI. Thus personal reasons, such as revenge on the former employer or the compulsion to consume child pornography, might lead to a person's commission of cybercrimes. Referring to Lusthaus, for others cybercrime (for example entering secured networks) replaces a hobby – cybercrime represents a pastime and offers the possibility to measure one's own skills and knowledge against like-minded people (Lusthaus 2013a: 47). Whereas hacktivists and cyberterrorists pursue political or ideological aims in committing cybercrime, Lusthaus refers to another group of persons for whom financial gain is the decisive reason for their action, and whose behaviour is merely profit-oriented. Finally, Lusthaus mentions perpetrators acting on behalf of states, so-called cyberspies. The author notes that the mentioned categories represent ideal types, but it is quite usual that in reality a combination of different motives can occur (Lusthaus 2013a: 47). Moreover, he assumes that the financial aspect is becoming increasingly the most important reason for the commission of cybercrimes, mainly since it appears as an alternative source of income, and that therefore even proper cybercrime careers are chosen (Lusthaus 2013a: 55).

A similar division of motivational reasons of cybercriminals is made by Koops (Koops 2010). Here the author refers, among other things, to a typology by Rogers, in which the motivation of cybercriminals is divided into:

'1. revenge (against persons, organisations, countries, or continents); 2. financial gain; 3. curiosity (knowledge, sensation, intellectual challenge); 4. fame (media attention, boasting, popular hero).' (Rogers 2006 quoted in Koops 2010)

Further Koops names Thomas & Loader, who also classify cybercriminals based on the respective categories:

'Another relevant classification is based on different motivations. [...] distinguish between hackers and phreaks (motivated by curiosity), information merchants and mercenaries (motivated by financial gain), and terrorists, extremists,

and deviants (motivated by political or social activity).’ (Thomas & Loader 2000 quoted by Koops 2010)

Cross and Wall expand this list of motives with the factors ‘for fun’ and sexual incentive (Cross 2008 and Wall 2007 quoted in Koops 2010).

5 Organisational structures

What kinds of statements are evident in the academic literature regarding the organisational forms and structures adopted by cybercrime groups? Are cybercriminals fundamentally lone operators who occasionally offer criminal services? Are cybercriminals more likely to cooperate in the context of loose networks with flat hierarchies or do they rather operate within stable, job-sharing and hierarchically structured groups? Only few scientific scholars are concerned with cybercrime groups and their organisational structures (Lusthaus 2012: 72 et seq., Leukfeldt 2014, Leukfeldt 2015). Moreover, only a small percentage of the statements are based on empirical research which clarifies that, from a scientific point of view, there is a need for additional research.

‘There is a lack of systematic research about the nature of criminal organizations active in cyberspace.’ (UNODC 2013: 39)

5.1 Lone operators versus organised groups

There are contradictory accounts in academic literature with regard to the question as to whether organised cybercrime actually exists.

Many authors affirm that cyber offences are predominantly committed by lone operators, meaning that organised cybercrime is an exception and that cooperation between cybercriminals can only be of short duration. According to their point of view, a job-sharing course of action in cyberspace is neither necessary nor effective.

Brenner for instance refers to the fact that until 2002 there is no reference as to whether organised criminal actions can possibly occur in cyberspace and, if organised criminal actions can arise in cyberspace, as to the question of which development this might take (Brenner 2002: 24 et seq.). The lack of discussion on organised cybercrime can, according to Brenner, on the one hand be explained by the general perception of cybercrime being connected to hackers who, as mavericks, do not tend to engage in criminal groups. On the other hand, the individual perpetration seems to be proven by the fact that

until 2002 the majority of public cybercrimes seemed to be committed by lone operators (Brenner 2002: 26 et seq.).

At the beginning of this century, Nisbett, too, asserted that there was a lack of visible organised cybercrime and he deduced that it was therefore legitimate to ask the question as to how likely collective and job-sharing cooperation would emerge in cybercrime (Nisbett 2002, cited in McCusker 2006: 8).

Furthermore, the ICT facilitating the course of action for individuals is perceived as the main reason cybercriminals can operate by themselves and are not dependent on accomplices. Wall points out that owing to the internet, it is possible for a single person to execute many minor criminal acts automatically, simultaneously making profits the size of those gained by larger groups of perpetrators, whereas the risk of being spotted remains fairly low.

'[...] the internet has transformed the organization of crime in substantially different ways to the organization of more traditional crimes. In a nutshell, networked technologies create an environment in which there is no need to commit one large risky crime anymore because one person can now commit many small crimes with lesser risk to themselves.' (Wall 2014: 228)

Furthermore, the anonymity in cyberspace may also function as an explanation as to why cybercriminals tend to work alone, rather than in an arrangement with others. The difficulty of creating and investigating reliability in this anonymous space gives rise to the suspicion that many perpetrators are not willing to cooperate with other unknown people via cyberspace, since the basis of cooperation would have to be trust.

'But anonymity does not only offer protection, but also presents a number of challenges. Where one does not truly know whom one is doing business with, it makes it difficult to assess trustworthiness or to retaliate should dealings go sour and agreements need to be enforced. This creates a large deficit of trust [...]. With such challenges, it would seem unlikely that a high level of collaboration would take place in the world of cybercrime. In an online world defined by such anonymity, it would be expected that cybercriminals would often act alone.' (Lusthaus 2012: 71)

In the status report on Organised Crime in 2004, the Council of Europe states that the majority of cybercriminals act as lone perpetrators. The aforementioned seems to occur especially in CIA¹⁴³ offences, for instance in relation to hacking, spreading computer viruses, Trojan horses, and computer worms. There were also cases in which criminals joined forces with each other in crime areas such as internet fraud, credit card theft or internet blackmailing (Council of Europe 2004: 170 et seq.). Correspondingly, the possibility of co-

¹⁴³ Confidentiality Integrity and Availability of computer data and computer systems.

operation has to be differentiated depending on the respective cybercrime area. At the same time, the authors predict that there will be an important increase in organised cybercrime particularly in the field of e-commerce (Council of Europe 2004: 171).

Contrary to the assumption that cybercriminals predominantly act alone, there are a number of authors who, based on theoretical as well as empirical research, demonstrate that there is in fact cooperation between cybercriminals, as cooperation increases the probability of success and monetary profit. This cooperation differs in its level of strictness and duration. This view is also supported by members of the prosecution services:

‘But cybercriminals are not always lone operators who eschew collaboration. In fact, they are increasingly engaging in partnerships with others and are developing some degree of organisation in their criminal dealings. This has been acknowledged by law enforcement officers working in the area with regard to the cybercriminal operations they are encountering.’ (Lusthaus 2012: 71 et seq.)

Rather, the question as to whether criminals in cyberspace are more lone operators or act as part of a network or group should be less regarded as an antagonism, but rather as different stages in temporal development. On the basis of academic literature one can pursue the development from the ‘early stages’ of cybercrime, influenced by hackers acting alone, to the emergence of durable underground economies that regulate the trade of ‘cybercrime products’ and ultimately durable cooperation between cybercriminals with an entrepreneurial structure (Protalinski 2008).

Fitzgerald, too, marks the decline in the proportion of single perpetrators. According to him, the reason for this might be that some years ago hackers conducted every single step of a criminal act themselves, whereas cybercriminals today specialise in separate steps and as a consequence act entrepreneurially.

‘Just a few years ago, most hackers [...] handled all aspects of an operation, from phishing to building fake websites to cashing in on the fraud. Since then, cybercriminals [...] specialize, they create markets and above all, they’re entrepreneurial.’ (Fitzgerald 2009)

Lusthaus shares this thought and describes the specialisation and development of diverse criminal roles in cyberspace, putting this down to the fact that more and more criminals, who are notably less rooted in technical know-how and as a consequence more dependent on other criminals in cyberspace, are forcing their way into this offence field. As Lusthaus states, the increasing dependency of these new cybercrime actors on expert know-how leads to the trend that there are fewer lone perpetrators in cybercrimes who can carry out the criminal acts self-sufficiently. As a consequence, the cybercriminals form greater networks to carry out their crimes (Lusthaus 2012: 77 et seq.). Summing up, the skills and know-how of individuals getting involved in cyber-

crime affect the way the cooperation between cybercriminals is structured and organised (UNODC 2013: 42 et seq.).

‘The other important point to note is that what began as an industry centered on hackers, and those with high-level computer skills has now broadened to include a wide range of people who perform a wide range of functions. Elite-level hackers and computer operators certainly continue to exist, but others involved clearly have varying degrees of expertise. With such differentiation of roles, it is not surprising that contemporary cybercrime involves a significant degree of collaboration.’ (Lusthaus 2012: 77 et seq.)

In addition, UNODC also refers to the development from mainly single perpetrators to collaborations. Further it is assessed that this development is strengthened through OC groups further weakening the significance of single hackers in cybercrime.

‘[...] in a relatively short period of time, cybercrime has transformed from a low volume crime committed by an individual specialist offender to a common high volume crime, “organized and industrial like”.’ (UNODC 2013: 45)

Also with regard to an empirical study on illegal online marketplaces in which cybercrime tools and stolen data were sold, one can observe that cybercrime is committed in an organisational way. From the results they found, the authors concluded that in forums the percentage of cybercriminals being part of a network or group is today significantly higher than in the mid-2000s: the proportion of single perpetrators decreased accordingly from approx. 80 per cent to 20 per cent. Ablon et al. point out that this progression is connected to the division of labour accompanied by synergy effects that positively influence the criminal profits and are the reason for single perpetrators ending up in larger groups of criminals.

‘But while an individual is good at one thing, organizations (or well-coordinated groups of individuals) can combine many different skill sets to accomplish bigger goals with bigger returns. Thus, there has been a tendency for these organizations to grow, as individuals coalesce into bigger groups over time, albeit with exceptions.’ (Ablon et al. 2014: 4 et seq.)

Other authors also indicate that, similar to the offline world, collective actions in cyberspace seem to be more promising and effective than solo effort since amongst other things a vast level of organisation is required for carrying out a cybercrime (UNODC 2013: 39). Cooperation with other criminals in cyberspace is thus becoming more and more important.

‘Cybercrime often requires a high degree of organization to implement, and may lend itself to small criminal groups, loose ad hoc networks, or organized crime on a larger scale.’ (UNODC 2013: 39)

According to the authors, a very promising cooperation form comprises a ‘virus writer / coder / Web designer’, a ‘spammer’ and a ‘money launderer’.

Such a combination would allow professional, innovative and conspiratorial action (McCafferty 2004). The results of an empirical study by Lusthaus show that even the lack of social control amongst cybercriminals can be solved by adopting new mechanisms adapted to cyberspace (Lusthaus 2012: 71).

Moreover, the thesis that cybercrime is increasingly being conducted by networks or groups is also supported by various empirical studies. As an example, the Detica/BAE Systems study asserts that the majority – up to 80 per cent – of cybercriminals are part of a group or network and do not act as lone perpetrators (Detica/BAE Systems 2012). In support of this, in 2003 the American Federal Trade Commission identified an even lower percentage in the field of identity theft and internet fraud: less than 5 per cent of criminal acts were committed by single perpetrators (McCafferty 2004). Ultimately, the results from Lusthaus's empirical analysis confirm the fact that cybercriminals are cooperating increasingly: more than half of cybercrime investigations listed in press archives of the US Ministry of Justice clearly reveal indications of a job-sharing perpetration by the accused (Lusthaus 2012: 71 et seq.).

In summation, there is a visible development during the last two decades in the perception of whether cybercriminals manifest themselves as single perpetrators or as members of bigger job-sharing collaborations. Empirical research clearly shows that there is criminal cooperation in all fields of cybercrime. However, these results should not lead to a misconception that allows one to neglect the importance and number of lone perpetrators in cybercrime. It is mainly this combination of constantly newly emerging individual criminals on the one hand and already established criminals operating in groups on the other hand that makes cybercrime particularly obscure and dangerous (UNODC 2013: 46).

'At the global level, law enforcement respondents to the study perceive increasing levels of cybercrime, as both individuals and organized criminal groups exploit new criminal opportunities, driven by profit and personal gain.' (UNODC 2013: xvii)

'Overall, while criminal groups likely predominate in certain forms of cybercrime, it is clear that all typologies – including individual perpetrators – must be taken into account.' (UNODC 2013: 46)

5.2 The heterogeneity of organisational structures in cybercrime

Based on the aforementioned findings that prove cooperation between perpetrators in the online world, the question of how these criminals cooperate will be discussed in the following sections. Whereas some authors mainly de-

scribe the cooperation between cybercriminals as loose networks, there are also authors who argue that this cooperation exists as strong and lasting structures.

Lusthaus argues that, cyberspace being a relatively new phenomenon, one cannot expect exact replica of typical offline criminal organisation forms (Lusthaus 2013b: 59). In contrast, other authors favour the view that cybercriminals and their respective structures can indeed be seen in analogy to offline crime fields. In 2001, Grabosky expresses that cybercrime is 'old wine in new bottles'. Pursuant to his point of view is the internet's possibility of creating new methods for crime commitment; nonetheless, the offences themselves as well as the perpetrators' motives are analogous to crime in the offline world (Grabosky 2001). Broadhurst suggests the possibility that criminal structures that exist in the 'real world' are also duplicated in cyberspace, alleviating the aforementioned trust issues of cybercrime groups by copying practices used by offline networks (Broadhurst et al. 2013:16). Subsequently, UNODC, too, asserts that cybercriminals and cyber groups resemble those existing in the offline world and sometimes even meet requirements of strict offline OC definitions (UNODC 2013: 39 et seq.).

'There is no reason to think that the development of such typologies and approaches [like the UNODC typology of organised criminal groups or the Euro-pol definition of organised crime] cannot in some way be applied to the involvement of organized criminal groups in cybercrime.' (UNODC 2013: 40)

These findings lead to the suggestion that cyberspace consists of similar forms of cooperation to those already existent in the offline world. Accordingly, cyberspace should be marked by heterogeneous forms of criminality and cooperation, and as a consequence it should manifest strict, hierarchical forms of organisation, too.

'Cybercriminals [...] adopt various structures. The crime family model obviously still applies when the Mafia is involved. Some groups that seem independent of the Mafia, like the people who ran Carder's Market [...] also use a Mafia-like structure and terminology. Phishing groups tend to work like Japanese keiretsu [...]. Cybercriminals sometimes use a hub-and-spoke model, where a criminal mastermind puts together various tools and people needed to pull off a job [...].' (Fitzgerald 2009)

Two 'extremes' in academic literature regarding the level of organisation in cybercrime can be revealed: loose networks on the one hand and strictly hierarchical organisations on the other hand. How exactly this cooperation develops and what forms have been identified in between, will be elaborated on in the following paragraphs.

5.2.1 Loose networks versus structures

Academic literature often reflects the view that cybercriminals only cooperate in the framework of ‘loose structures’ based on specific projects. Therefore, this cooperation could not be compared to structures and working methods of OC groups and gangs in the offline world. Besides, it is assumed that while these groups have some kind of ‘pecking order’, they do not have a formal hierarchy. Hence, all members would be regarded as equal.

‘[...] many cybercriminal groups are small, loosely structured and without a clear agenda. [...] There was no formal hierarchy, only an informal pecking order, and orders could not be given. [...] Such groups have limited organisation in a broad sense [...]’ (Lusthaus 2013b: 57)

Regarding other cases, Lusthaus mentions ‘cyber gangs’ that contain a stronger hierarchy, although they will never attain the level of organisation of offline gangs owing to the intrinsic characteristics of cybercrime (Lusthaus 2012: 78 et seqq.):

‘In such cases [...] the leader of such a group might issue the order to carry out a DDoS to an underling or ask that person to engage someone who could carry out the attack for them. What should be noted, however, is that these sorts of cyber gangs have not reached and, due to the nature of online interactions, are unlikely to reach the level of organisation, cohesion and hierarchy of physical gangs.’ (Lusthaus 2012: 80)

In her publication from 2002 Brenner assumes that if cybercriminals collaborate in the future, their cooperation will be organised differently from, for instance, mafia organisations. Their organisation could be best described with Arquilla & Ronfeldt’s¹⁴⁴ concept of ‘swarming’ which consists of a series of changing coalitions between single perpetrators or small, content-oriented criminal cooperation. These ‘manoeuvre units’ are composed of two to six individuals and echo gangs from the offline world. The leadership of such units is assumed to be more egalitarian compared to gangs in the offline world as the members have acquired similar technical skills. Furthermore, Brenner states that the criminal career of cybercriminals, contrary to the career of criminals in the offline world, is less dependent on the ‘success’ of the network, since relevant technological know-how would allow the criminal to continue alone if necessary. According to Brenner, this means that a member can leave the group at any time, which is the reason why there is no development of rigid and hierarchical leadership structures within the group (Brenner 2002: 43 et seqq.). Against this background, the author concludes that cooperation in cyberspace does not adopt a formal and hierarchical organisation;

¹⁴⁴ Arquilla & Ronfeldt 1997: 8 et seq.

instead it mainly manifests itself as loose and temporary networks (Brenner 2002: 50).

‘Instead of multi-generational criminal enterprises, cybercriminal organizations will emphasize arm’s length, instrumental associative alliances.’ (Brenner 2002: 47)

Europol, in the 2011 ‘Threat Assessment report’, states that especially when it comes to internal hierarchy, cybercrime groups can be perceived as the complete opposite of the traditional OC concept. As stated by Europol, cybercrime groups are often not equipped with a visible leadership and the division of labour depends on the technical skills of members who know each other mostly only online (Europol 2011: 6). ‘The Internet Organised Crime Threat Assessment’ (iOCTA), another Europol report from 2014, stresses that the actual form of organisation of cybercrime groups is rather temporary.

‘Relationships between cybercriminals are often transient or transactional and although they may form more coherent, project-based groups, they lack the structure and hierarchy of a traditional organised crime group.’ (Europol 2014: 9)

Based on empirical results Broadhurst comes to the same conclusion: criminals, regardless of whether they operate online or offline, tend to collaborate rather in loose networks than in formal organisations (Broadhurst et al. 2013: 19). In this context McCusker states the assumption that cybercrime groups do not differ significantly from traditional organised crime inasmuch as they, too, are increasingly divided into smaller, horizontal subgroups.

‘It is recognised that in fact, flatter, more horizontal networks, comprising cell-like ‘crews’, have become the norm in much of the organised crime environment (though Chinese triads and Japanese yakuza have remained traditionally hierarchical in nature).’ (McCusker 2006: 8 et seq.)

The swarm concept as a loose and temporary cooperation of cybercriminals is further picked up on by UNODC:

‘The internet and related technologies lend themselves well to broader coordination between individuals across a dispersed area – opening up possibilities for shorter-lived “swarm” criminal associations, and divergence from traditional models such as standard and regional hierarchy-based groups.’ (UNODC 2013: 45)

The statement of hierarchies not being necessary in cybercrime groups owing to cybercrime’s nature is further advocated by various authors. Tropina argues that in respect of the perpetration of cyber offences, hierarchical forms of organisation are as insignificant as a vast amount of perpetrators. Cybercrime groups are, in the opinion of the author, rather comparable to modern enterprises whose success largely depends on the high quality of the technological

tools used (Tropina 2012: 162). In addition, Wall affirms that formal hierarchies, in terms of a 'command and control' model, are of less importance for cybercrime groups, as their form of cooperation rather resembles a 'Wiki model'.

'So we find that cybercrime is increasingly taking on a 'Wikicrime' form of peer-production, for want of a better description (after Tapscott and Williams 2007), as its organization follows a Wiki model of organization characterized by online collaborations rather than the "command and control" Mafia model that is assumed by many.' (Wall 2014: 231)

5.2.2 Online platforms as an organisational vehicle

Despite the widespread assumption of cybercriminals cooperating in loose networks, there are more and more indications in the literature that point to the significance of illegal online platforms in relation to both structural and stable cooperation between cybercriminals, as well as the formation of new groups.

Such a development is supported by illegal forums and marketplaces in the Clearnet/Surface Web, deep web or darknet amongst others, as they simplify the cooperation between cybercriminals (Glenny 2012: 62 and 65). Illegal platforms grant criminals the possibility to both communicate and recruit new members. Besides, they function as stable and mostly anonymous communication channels and ensure confidence building and sanctioning through internal forum mechanisms. They facilitate and structure the cooperation between criminals in allowing them to come together easily and cooperate on a project basis. Apart from this, the marketing and selling of crimeware components are enabled through online forums, too. Offers include 'tutorials' by means of which 'prospective cybercriminals' can learn the technical know-how (Europol 2011: 6).

The 2011 report of Group IB on the Russian cybercrime market reflects the fact that illegal online marketplaces and forums facilitate cooperation between criminals, even leading to the formation of new organised cybercrime groups. The following trends have been identified by the above-mentioned report: firstly, the consolidation of various market participants resulted in an emergence of larger, hierarchically structured cybercrime groups. The authors interpret this emergence as a plain example of the avoidance of unorganised cooperation in favour of the establishment of centralised structured groups. Secondly, a reinforced exchange and mutual support in committing offences between the different cybercrime groups were identified (Group IB 2011: 7).

The question as to whether illegal online platforms by themselves are to be understood as some sort of criminal group or merely as 'rooms' for cyber-

criminal cooperation is regarded differently in academic literature. What many authors can agree upon is the opinion that such forums have a clear division of labour and sophisticated organisation. Lusthaus for example mentions that illegal online marketplaces are often characterised by a strong hierarchical structure (Lusthaus 2012: 80). UNODC describes these forums as a 'social network of individuals engaged in organized criminal activity' (UNODC 2013: 47). Key positions, which other agents gather around, are held by a few individual perpetrators or small groups (for instance malware programmers and botnet C&C owners) (UNODC 2013: 47 et seq.).

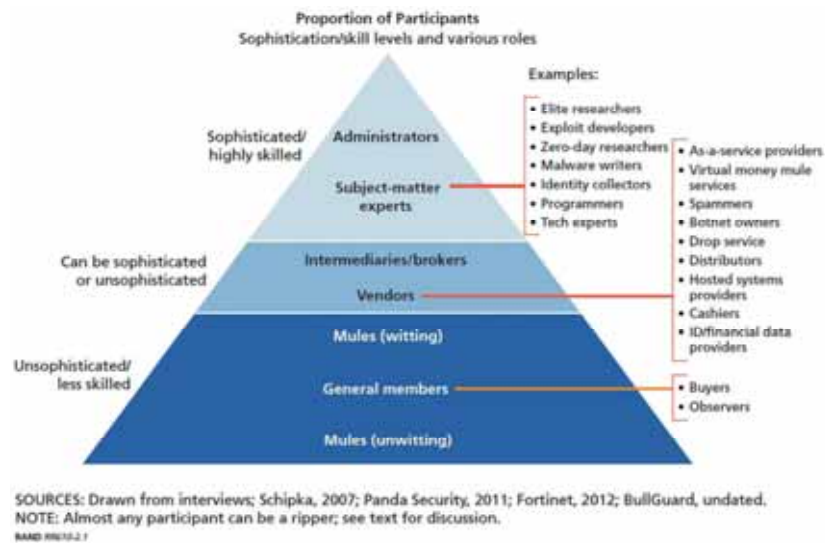
In their study on 'black markets',¹⁴⁵ Ablon et al. were also able to show that underground marketplaces are frequently organised hierarchically. This hierarchical structure is accordingly reflected, amongst other things, in the division of criminal income. Hence the higher a participant is ranked in the internal hierarchy of the market, the higher the profit he receives. Furthermore, the authors highlight that different levels of hierarchy obtain different and varying strict codes of conduct and access (Ablon et al. 2014: 5). Moreover, it is assumed that underground marketplaces can, similar to traditional economic systems, be divided into the basic categories of sellers (supply), buyers (demand) and intermediaries. According to the authors of the study, the intermediaries obtain a central role: they operate as an independent third party controlling and confirming products and participants, thus simplifying transactions and ensuring a certain form of security and reliability (Ablon et al. 2014: 5). The authors also claim that within the underground marketplaces specific roles can develop (cf. figure 1). Hence, the administrators are located at the top. Correspondingly, the subject-matter experts follow, who possess sophisticated technical knowledge in the most diverse fields (root kit creators, data traffickers, cryptanalysts, etc.). The level below this is composed of intermediaries, brokers and vendors who are also experienced, although in a less extensive way than the administrators and subject-matter experts. Lastly, the lowest levels consist of general members and, ultimately, of mules who are intentionally (and in an organised way) or unintentionally involved in criminal activities (Ablon et al. 2014: 5).

As is notably illustrated by the authors, the number of users of underground marketplaces will prospectively increase. This is, on the one hand, reinforced by the rapidly growing number of websites, forums and chat channels and, on the other hand, by the fact that 'digital natives' are at lower risk of fearing contact with technical challenges. Also the number of highly qualified parti-

¹⁴⁵ 'Black markets are organized and run for the purpose of cybercrime; they deal in exploit kits, botnets, Distributed Denial of Service (DDoS), attack services, and the fruits of crime (e.g. stolen credit card numbers, compromised hosts)' (Ablon et al. 2014: 1).

cipants has, according to the authors’ view, undergone a rapid increase in the past few years. Consequently, the quantity and quality of services has increased drastically (Ablon et al. 2014: 5 et seq.).

Figure 1: Different levels within underground marketplaces



Source: Ablon et al. 2014: 6

Lusthaus confirms the hierarchical division of underground marketplaces. At the top, he places the administrator who is in charge of the site. Subordinate to the administrator are moderators who are responsible for the maintenance and enforcement of the rules within the marketplace or the forums. Further down there are various members of different statuses and diverse privileges. The hierarchical rise of a forum member is possible if the member manages to provide trustworthiness and skills (Lusthaus 2012: 80). UNODC, too, refers to divergent allocations of roles and responsibilities within these online forums (UNODC 2013: 46 et seq.).

‘A cybercrime “black market” has been characterized in which groups and individuals with different roles and sometimes acting in multiple roles (including “programmers”, “distributors”, “technical experts”, “hackers”, “fraudsters”, “hosters”, “cashers”, “money mules”, “tellers” and “leaders”) interact in the process of malware creation, computer infection (such as through phishing emails), botnet management, harvesting of personal and financial data, data sale, and “cashing-out” of financial information.’ (UNODC 2013: 46 et seq.)

According to Europol, these forums are, however, neither part nor a catalyst of organised crime; they merely coordinate criminal relationships between cybercriminals (Europol 2014: 20). It is estimated that this kind of ‘underground economy’ could be an example of how ‘serious crime’ might be structured in the future (Europol 2014: 20).

Europol shows that the structuring and organising functions of these forums can pose an important threat: they ease and promote exchange between, on the one hand, inexperienced amateurs who incidentally occupy themselves with cybercrime and, on the other hand, highly qualified cybercrime experts. This interplay is thought to be a vicious circle leading to the qualitative and quantitative increase of cybercrime in the future (Europol 2014: 23).

Décary-Héty & Dupont claim that the process of being promoted to a higher level in the hierarchy or even contacting people from the higher ranks can often be very protracted. According to the authors, preconditions include long, intensive participation in the forum as well as earning a reputation that depends on the reliability of every member in their provision or payment of services (Décary-Héty & Dupont 2013: 6 et seq.).

Peachey alludes to the network ‘CarderPlanet’ as an example of a strictly organised online forum that resembles the conceptualisation and structure of the Cosa Nostra: to prevent the members from betraying each other, a quality control system was established (Peachey 2014).

‘Roman Vega was the administrator of CarderPlanet that was set up along the lines of La Cosa Nostra, with a Godfather and a number of Dons – including Vega – one rank down. Under Vega’s control, CarderPlanet became one of the busiest online marketplaces for the sale of stolen financial information, hacking and laundering services, with more than 6,000 members. He set up a quality control system for sales of credit card information to ensure that the fraudsters weren’t ripped off by their fellow fraudsters.’ (Peachey 2014)

Recently Leukfeldt (2015) published research on theoretical frameworks and organised cybercrime. His work deals with different types of cybercriminal networks and the role of meeting places in the development of these networks. He points to research on organised crime where social ties and social opportunities are important in the formation and functioning of criminal networks and examines whether these theories also apply to cybercriminal networks (Leukfeldt 2015: 93). While ‘several case studies show that the Internet provides an opportunity structure for decentralised, flexible networks of loosely organised criminals who collaborate and distribute work based on knowledge and skills’ (Leukfeldt 2015: 95), ‘several studies describe that just as in traditional networks, there are still important actors (nodes) with a role as a bridge builder’ (ibid.: 96). Empirical research indicates that just as with traditional organised crime, ‘social relationships may be important for the re-

cruitment and growth of cybercriminal networks', however getting new contacts in the virtual world can arise faster. This is where forums, functioning as offender convergence settings (Felson 2003, cited in Leukfeldt 2015: 97), have an important role in facilitating the growth and development of networks. These settings provide a structure and continuity where 'newcomers can come into contact with criminals, enter existing criminal networks or form new criminal alliances' (Felson 2003 and 2006, Von Lampe 2009, cited in Leukfeldt 2015: 97). The question remains as to the extent to which cybercriminal networks make use of these forums, as another study by Leukfeldt (2014) shows that social ties and relationships in a network of cybercriminals can also be based on real-world social networks rather than on internet forums.

5.2.3 Structures in cybercrime

Despite many presumptions, the study by Detica/BAE Systems shows that by no means are all cybercrime groups composed of members who only collaborate temporarily and relatively loosely without constituting a formal hierarchy. The study's editors were able to identify numerous cybercrime groups significantly resembling traditional OC. Hence some of those strictly organised groups consist of a core group comprising experienced online criminals who do not personally commit the offences, but rather delegate the task to other members. In this way, multiple teams with several tasks are created. For instance one team would produce malware and another team would spread the malware on the internet while a third team would execute the purchase of needed data. This 'division of labour' is reported to allow a certain degree of specialisation within the group with the result that every group member would only need to be an expert in his/her own field of specialisation. Therefore, the authors claim that cybercrime can be conducted more easily in cooperation with other group members, thus combining their personal areas of specialisation (Detica/BAE Systems 2012). Tropina, too, refers to cybercrime groups often being lead by internal core groups which themselves do not directly commit the crime, but instead function as distributors of tasks to members in the group (Tropina 2012: 163).

'For instance, the first group writes a malicious code, such as a 'Trojan'; the next group is responsible for the distribution and use of the malicious software on the Internet; yet another group collects data from the illegal platforms and prepares everything for the identity theft.' (Tropina 2012: 163)

Tropina moreover identifies so-called 'elite criminal groups' (Tropina 2010: 2) that form a closed network and are not in need of participating in online forums. As reported by Tropina, these groups are able to conduct the entire process of committing cyber offences on their own, since they possess sub-

stantial resources themselves. Hence, the participation of outsiders or recruiting experts into the network would not be crucial (Tropina 2010: 2).

By means of a network analysis Décary-Héту & Dupont examined a group of ten hackers and were able to prove a sophisticated and strongly organised form of cooperation together with a strict hierarchy: the hackers lived in different Canadian cities, never made contact with each other in person and only fostered relations via ICT. In the course of the study it was concluded that the previously mentioned group formed the highest hierarchical rank of a network containing 771 chat participants. Through intermediaries, who form the centre in chat communication, the hackers of highest rank communicated with other members. Consequently, the network analysis revealed that people who at first sight appear to be outsiders within the online community actually hold a significant position for the criminal network. Moreover, it was proven that members with multiple contacts did not always function as central characters (Décary-Héту & Dupont 2012: 161 et seq.).

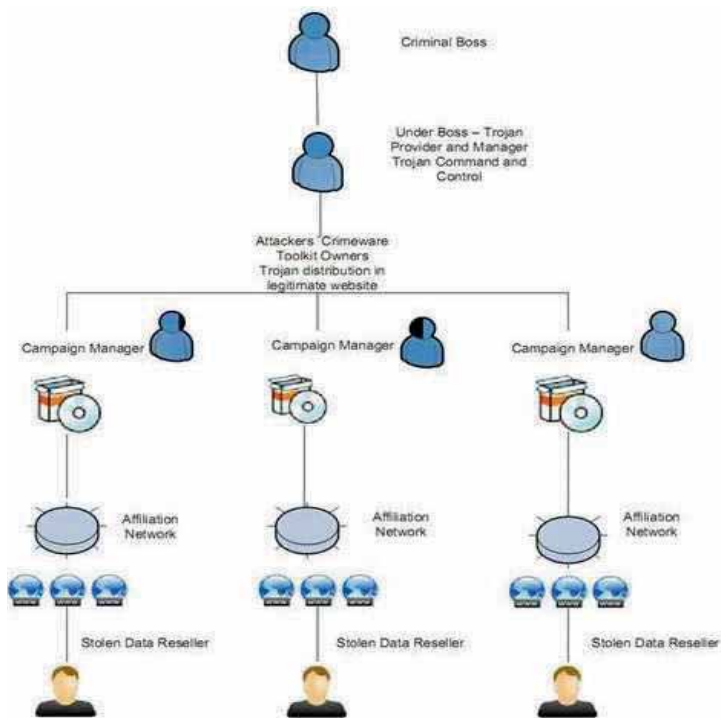
Other cybercrime groups resemble internationally operating enterprises with regard to their organisational and hierarchical structure. In 2008 Protalinski advocated the theory that rapidly growing cybercrime enterprises that make vast amounts of profits are about to emerge. Regarding the hierarchical structure, every 'employee' would carry a specific role, while the payment is based on an elaborate system of remuneration. Protalinski further claims that cybercrime enterprises are capable of developing a successful business concept by performing selective attacks on financial institutes, enterprises, and government agencies as well as through the excellent handling of stolen data (Protalinski 2008).

Finjan,¹⁴⁶ a cybersecurity company, compares the employee organisational chart of some cybercrime enterprises with traditional mafia structures (figures 2 and 3). In both cases there is a 'boss' who acts as an entrepreneur and who does not personally commit the (cyber)crimes. Under the boss's command, the 'underboss' leads the operations and occasionally provides the tools for committing them. In traditional mafia organisations, there exist various 'capos' or lieutenants that are subordinate to the 'underboss'. They lead their own 'soldiers' and hold responsibility for parts of the operations. Regarding cybercrime, Finjan refers to the lieutenants as 'campaign managers' who, with the assistance of their subordinate networks, perform cyberattacks aiming at data theft. The stolen data is resold by 'resellers' who mirror the 'associates' in mafia organisations. As they were not involved in the actual cyber

¹⁴⁶ Finjan's second quarterly report in 2008 refers to data gained by the Malicious Code Research Center (MCRC), which specialises in detecting dangerous vulnerabilities that can be exploited to conduct malicious attacks (Protalinski 2008).

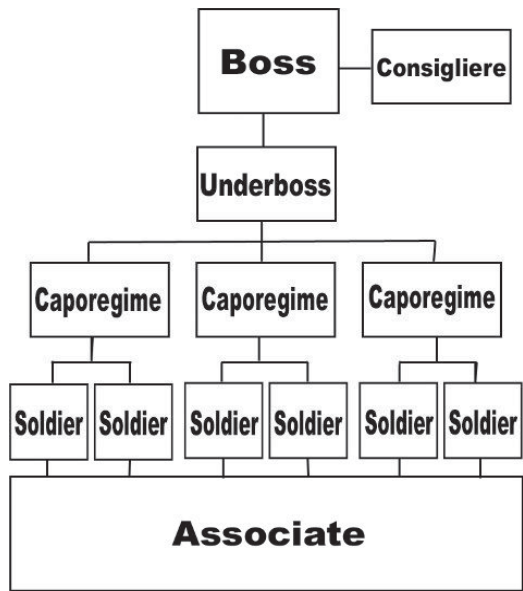
offences, they cannot trace the way the data was stolen, although they are assumed to be familiar with the codes of conduct within the groups (Protalinski 2008).

Figure 2: The hierarchy of the ‘Digital Mafia’



Source: Finjan, cited in Protalinski 2008

Figure 3: Traditional mafia structure



Source: Figure based on Klaus von Lampe, <http://www.organized-crime.de/organisiertekriminalitaet.htm>

5.3 Typology of cybercrime groups

Beyond the question of the extent and the forms of organisation in cyber-crime, various authors deal with the typology of cybercrime groups. One example is the study ‘Organised crime in the digital age’ by McGuire, which elaborates on the typology based on the objective – mainly online; online and offline; mainly offline – as well as on the level of organisation – less organised; more organised.

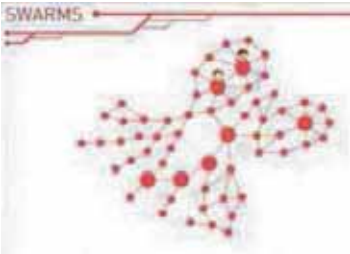

Accordingly, the cooperation between cybercriminals can be divided into the following ‘types’ (cf. table 1):

- 1. Groups whose activities mainly occur in cyberspace and aim at online targets (type 1).
- 2. Groups who aim at online as well as offline targets (type 2).


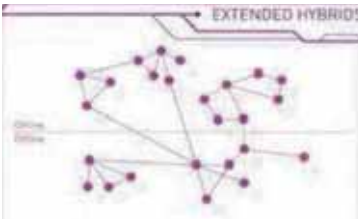
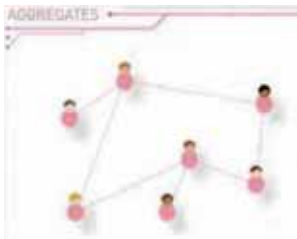
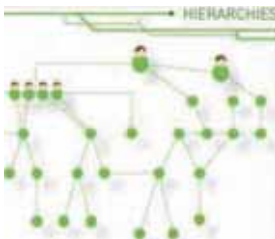
3. Groups who mainly act in and focus on offline fields, but make use of ICT in order to enlarge their criminal range (type 3) (Detica/BAE Systems 2012).

Type 1 groups, as reported by the authors, can be categorised into ‘swarms’ (low level of organisation, e.g. hacktivist groups) and ‘hubs’ (higher level of organisation, e.g. ‘scareware’ operations). While ‘swarms’ do not contain any visible chain of command and frequently consist of amateurs and only include ‘weak member controls’, ‘hubs’ make use of clearly structured chains of command and key members as well as strict admission procedures (UN-ODC 2013: 46). Type 2 groups are divided into ‘clustered hybrids’ (low level of organisation, e.g. carding forums and skimmers) and ‘extended hybrids’ (higher level of organisation such as telephone theft and online trade). Type 3 groups, on the other hand, could be classified under ‘aggregates’ (low level organisation, e.g. street gangs) and ‘hierarchies’ (higher level organisation, e.g. traditional mafia).¹⁴⁷ McGuire assumes that hybrid groups are the most successful ones because they have learned to combine online and offline activities leading to a convergence of new and old forms of criminality (Detica/BAE Systems 2012).

Table 1: Typology of cybercrime groups

Targets	Groups with a lower level of organisation	Groups with a higher level of organisation
Online (type 1)	<p>‘Swarms’ Groups that are organised like decentralised and network-like swarms without any direct chain of command. The most important connection is a common target. Crimes are mainly committed on-line.</p> 	<p>‘Hubs’ Functional groups consisting of smaller core groups whose members are further connected to a periphery of criminal accomplices. Within the core group, a formal hierarchy is established.</p> 

¹⁴⁷ A full explanation of the typology is made by Broadhurst, Grabosky, Alazab & Chon 2014.

Targets	Groups with a lower level of organisation	Groups with a higher level of organisation
Online and offline (type 2)	<p>'Clustered hybrids'</p> <p>Groups with few members who specialise in committing specific crimes, at specific places or with specific methods in virtual as well as non-virtual environments. They are composed of a decentralised structure.</p> 	<p>'Extended hybrids'</p> <p>Groups with a higher level of organisation. All subgroups are more or less of the same importance for the criminal activities. Crimes are committed online as well as offline.</p> 
Offline (type 3)	<p>'Aggregates'</p> <p>Groups from a non-virtual environment such as street gangs or thieves who continue to commit their crimes offline, although using ICT for support.</p> 	<p>'Hierarchies'</p> <p>Clearly divided groups with a strict, formal hierarchy (e.g. 'crime families') who commit crimes in a non-virtual environment and use the internet for support.</p> 

Source: Detica/BAE Systems 2012, authors' illustration

5.4 Size of cybercrime groups

According to the Detica/BAE System study, 50 per cent of the investigated cases of cybercrime include six or more perpetrators and in one quarter of these cases the groups were composed of 11 or more offenders (Detica/BAE Systems 2012). Further estimations about the size of cybercrime groups are made in academic literature and range up to several thousand members.

‘Concerning the size of the cybercrime groups (or networks), the estimates vary from 10 to several thousand members, when the affiliated networks are incorporated into the bigger and more complex structures.’ (Tropina 2012: 163)

Yet the size of a cybercrime group does not correlate with the damage caused. As previously mentioned in chapter 2, the use of ICT enables even individual offenders or small groups to carry out automated procedures and attain high illicit returns from a multitude of victims (Detica/BAE Systems 2012).

6 Involvement of organised crime in cybercrime

Since 2001, international prosecution authorities such as Europol, Interpol, UNODC and the International Narcotic Control Board (INCB) have been emphasising that traditional OC is linked to cybercrime (Lavorgna 2015a: 40 and UNODC 2013: 44 et seq.). Accordingly, traditional OC groups are one of various actors in cyberspace alongside lone operators, cyberborn groups, intelligence agencies, hacktivists, and others (Broadhurst et al. 2013: 19 et seq.).

Despite evidence that OC groups use ICT to commit offline as well as online crimes, there is so far, according to Broadhurst, little reliable information regarding the extent or percentage of OC involvement in cybercrime (Broadhurst et al. 2013: 24). Moreover, the quantitative determination would be dependent on the specific definition of OC and cybercrime (UNODC 2013: 44). Furthermore, the criminological research on the question of how the involvement of OC groups in cybercrime takes place empirically is not complete: one would have to examine the committed crimes,¹⁴⁸ the procedure and the organisation of criminal groups (UNODC 2013: 45).

Some authors doubt an involvement of OC in cybercrime. One thesis claims that OC groups are not reliant on cybercrime or do not possess the necessary technical skills to commit cybercrime (McCusker 2011: 108).

‘However, it remains unclear, and indeed doubtful, whether currently there are traditional organised crime groups operating within the cyber environment.’ (McCusker 2011: 116)

¹⁴⁸ In the following fields of offences an involvement of traditional OC has been detected: human trafficking, identity theft (e.g. credit card forgery), DDoS attacks on homepages for instance of gambling providers, drug trafficking, arms trade, pharmaceutical crime, child pornography, copyright infringement, industrial espionage, competition spying, money laundering via online systems of payments, etc. Indications of spheres of activity are mostly provided by cases publicised in the media, rather than by empirical studies (Bundesamt für Sicherheit in der Informationstechnik: 23; Benda 2011: 85; Choo & Grabosky 2013: 5 et seq.; Choo & Smith 2008: 39; Lavorgna 2013: 42; Lavorgna 2015b: 2; McCusker 2006: 12; McCafferty 2004: 2; Schönbohm 2014: 3).

Others suppose that forms of organised cooperation in cyberspace cannot be attributed to traditional OC groups, but rather to cyberborn structures:

‘Cybercrime has become an integral part of the transnational threat landscape and more recently, the concept of ‘organised crime’ has been attributed to cybercriminality. There has been subsequent disagreement and confusion concerning whether such crime is a derivation of traditional organised crime or an evolution of such crime within the online space.’ (McCusker 2011: 107 et seq.)

Lusthaus assumes that specific cybercriminal groups are fairly keen to use mafia terminology to describe their own group structure and for instance appoint mafia titles to members even though no hierarchical structure is visible. These groups are, as Lusthaus states, not to be compared to OC in the traditional sense, but rather defined as ‘mafia-like groups’ who try to create a myth (Lusthaus 2013b: 57). The following differences between organised cybercrime and traditional OC are accordingly detectable: while e.g. traditional OC groups resort to violence to regulate and control various offline marketplaces, in a virtual environment violence is not necessary. The possible sanction mechanisms to practise pressure and control, such as the exclusion from forums or a DDoS attack, are in general less violent than the execution of physical violence (Lusthaus 2012: 93 et seq.). Another important aspect of traditional OC groups that is only partly transferable to cybercrime is the control of territory. In cyberspace, an international environment without any borders, it is more challenging to maintain this control and new technical ways are necessary (Lusthaus 2013b: 58 et seq.). The author also mentions variations regarding the level of solidarity among members of criminal groups. Within cyberspace, it is hypothesised that upholding the group identity is very difficult, especially if the identity is put under pressure (Lusthaus 2012: 92 et seq.).

Other publications emphasise that there logically has to be an involvement of OC in cybercrime, as ICT provides plenty of possibilities and chances for OC groups, such as aiding the execution of traditional crimes and the concealment of assets. However, this involvement might not be perceptible at first glance.

‘Internet technology increasingly facilitates a wide range of serious and organised crime activity as a communication, research, logistics, marketing, recruitment, distribution and monetarisation tool.’ (Europol 2011: 3)

By comparison, cybercrime enables criminals to make multiple profits at the same time as it provides anonymity as well as a fairly low risk of being prosecuted (McCafferty 2004). Consequently, for McCusker, it is only logical that traditional OC is similarly involved in cybercrime as it usually is when it comes to any low-risk, lucrative ‘business area’.

'Logic would dictate that traditional organised crime groups will engage with cybercriminal endeavours as fervently as they will with any low risk, high profit non-virtual criminal activity.' (McCusker 2011: 108).

Pool-Robb similarly considers the advantages of cybercrime for OC groups: whereas criminals previously would rob a bank at high personal risk with the possibility to carry off five-figure amounts, criminals are now able to anonymously loot foreign bank accounts via PCs in other countries. In this way, they are able to hundredfold the profit without becoming the target themselves (Poole-Robb 2015).

'Professional criminals across Europe are forsaking traditional crimes such as armed robbery, muggings and burglary in favour of committing crimes on the Internet, where their chances of being caught range from slim to zero.' (Poole-Robb 2015)

Lavorgna views the realisation of traditional OC in cybercrime slightly differently and highlights that traditional OC groups are not actively participating in all offence fields of cybercrime, stressing that the use of the internet for criminal purposes is a generational issue. With regard to their traditional criminal activities, OC is speculated to fall back upon the conventional working methods of the offline world. In particular, with established OC groups the strategies and contacts are estimated to operate well together so that there would not be any need for tactical change (Lavorgna 2014: 265). The advantages stemming from an internet-based commission of offences (cf. chapter 2) can, in those cases, not outweigh the advantages (e.g. personal contacts) of the traditional commission of offences. Outside of its usual activity fields, on the one hand, OC continues to rely on proven personal contacts but on the other hand, OC is suspected of having recruited 'counsellors' who contribute their technical know-how for instance in the area of online money laundering (ibid.: 265). In this case there is, referring to Wall's typology, a 'hybrid crime' that combines the advantages of the virtual and non-virtual environment for the commission of crime (Wall 2007: 45 et seq.). As reported by Lavorgna, the example of trade in counterfeit pharmaceuticals, however, shows that there can also be a cooperation of traditional OC groups with organised cyberborn groups and not only with individual cybercriminals. Although the production of counterfeit pharmaceuticals is expected to remain in the hands of criminal networks, the distribution of medicine via online pharmacies would be managed by cybercriminals (Lavorgna 2015b: 232 et seq.). Lavorgna observes that illegal gambling¹⁴⁹ in cyberspace is already in the hands of

¹⁴⁹ Lavorgna in her thesis moreover analyses the importance of the internet in the offence fields of pharmaceutical crime, human trafficking with the purpose of sexual exploitation and drug trafficking (Lavorgna 2013).

OC groups: they manage online gambling sites or they blackmail providers of gambling homepages by means of DDoS attacks. According to Lavorgna it is mainly groups of younger members that participate in cybercrime (Lavorgna 2015a).

In agreement with Grabosky, there is no doubt that for some time now OC groups, when carrying out crimes, resort to ICT for maximising the profit and minimising the deposit (Grabosky 2007: 13 et seq.) and are therefore involved in cybercrime in a broad sense (Europol 2014: 22 et seq.). This development was already mentioned in 2004 by the Council of Europe and in a UNODC report from 2013:

‘Organised crime groups are especially involved in acts of sophisticated computer fraud, credit card fraud, and telephone fraud. Computer data stored and transmitted in encrypted form are also used by drug and arms dealers to carry out their activities. It is assumed that in future, electronic money transactions and “cyber money“ will be increasingly used for illegal gambling and for money laundering on the Internet.’ (Council of Europe 2004: 119)

‘Many cybercrime acts require a high degree of organization and specialization, and it is likely that the level of involvement of conventional organized criminal groups in cybercrime is high – at least in financial-driven cybercrime acts such as computer-related fraud, forgery and identity offences.’ (UNODC 2013: 44)

Consumer fraud would accordingly be the central field of activity in cyberspace for OC groups. The internet is presumed to ease the disposal of stolen or other illegally obtained goods (Council of Europe 2004: 120). Furthermore, the Council of Europe assessed in 2004 that OC groups on a larger scale were involved in content-related crimes. According to insights from the Council of Europe, the biggest part of the production and spreading of child pornography lies with organised crime (Council of Europe 2004: 121). Another relevant source of income is assumed to be the trade of pirated products (Council of Europe 2004: 123) as well as the illegal trade of drugs and pharmaceuticals only available on prescription (Council of Europe 2004: 120). The same report also suggests that OC is actively participating in online gambling with the purpose of laundering their money (Council of Europe 2004: 122).

The accomplishment of technically more complex cybercrimes, especially cybercrime in a narrow sense, does not pose a vast challenge for traditional OC, since corresponding services can be bought effortlessly; e.g. in the framework of Crime-as-a-Service (Peachey 2014).

‘[...] traditional organised crime groups are now able to step into cybercrime by purchasing bespoke skills and tools to support their criminal business.’ (Europol 2014: 5)

Consequently, the group members do not need to be technically experienced if the respective OC group has the money or influence at their disposal to be sure of getting support from third parties. McCusker also outlines that cybercriminals and OC can profit from one another because the skills and motivations complement each other. He assumes that traditional OC buys its way into committing cybercrimes by compensating for its lack of knowledge and skill by recruiting informants and service providers at universities or computer clubs. On the other hand, the cybercriminals get a chance to sell their skills. The cooperation between IT specialists and OC leads, in McCusker's opinion, to a new quality of cybercrime: while the OC groups contribute their criminal skills and contacts, the cybercriminals have attained the technical skills necessary for committing crimes in an automated way (McCusker 2006: 273).

To demonstrate this, a drug smuggling group operating in Belgium and the Netherlands until 2013, will be taken as an example. The group recruited various hackers who infiltrated the computer system that kept the movements and localisation of shipping containers in the harbour of Antwerp under surveillance. Thus, they could ship the narcotics in the shipping containers and manipulate the data of these specific containers in the logistics system, so that the drug smugglers were able to intercept the containers even before the shipping agents arrived (Europol 2014: 22 et seq.).

There is some evidence that OC groups are increasingly making use of forums and marketplaces on the deep web and darknet to contact cybercriminals.

'Traditional organised crime groups (OCGs), including those with a mafia-style structure are beginning to use the service-based nature of the cybercrime market to carry out more sophisticated crimes, buying access to the technical skills they require.' (Europol 2014: 11)

The purchase of criminal services by OC groups is not necessarily seen as dependence on cybercriminals, for some authors claim to have detected the entry of OC groups in technically sophisticated cybercrime (cybercrime in a narrow sense):

'Organised criminal groups are gradually moving from traditional criminal activities to more rewarding and less risky operations in cyberspace. While some traditional criminal organisations are seeking the cooperation of e-criminals with the necessary technical skills, newer types of criminal networks operating only in the area of e-crime have already emerged.' (Tropina 2010: 1)

The translocation processes described by Tropina are restated in the report by Group IB in which the Russian underground marketplace was investigated. They saw that traditional OC groups discovered online forums and marketplaces for themselves and not only in relation to the collection of illegally

earned money, but also the whole process leading to the cashing of the money. The authors infer that the aforementioned facts lead to a fusion of the online and offline world, which results in a decrease of investments in traditional fields such as prostitution or drug and weapon trade and an increase in cybercrime investments (Group IB 2011: 7 and Essers 2012). Other authors, too, note that the Russian mafia is undoubtedly involved in cybercrime in a narrow sense.

‘The Russian Mafia are the most prolific cybercriminals in the world. Organized cybercrime is a truly international affair, but the most advanced attacks tend to stem from Russia.’ (Goldman 2011)

The oldest and largest Russian OC group that is actively participating in cybercrime is, with reference to Goldman, the Russian Business Network (RBN). Generally, powerful OC groups that take a stake in cybercrime pose a special threat, since they possess a multitude of loyal, professional members as well as extensive financial resources (Goldman 2011).

‘Where hacktivists lack patience and most fraudsters lack skill, organized crime syndicates like the RBN possess the necessary tools to hack just about any target they set their sights upon. [...] Once a hacker in an organized crime unit has gained entry to a targeted system and reached the limit of his expertise, he’ll send the hack up the chain to a more expert attacker. That continues until it reaches an organization’s top hacker, who will often steal whatever information the organization wants and cover the previous hackers’ trails.’ (Goldman 2011)

Besides Russian OC groups, traditional OC groups from Romania have also found their way into cybercrime, as stated by an FBI agent (Fitzgerald 2009). Already in 2004, US investigating authorities mentioned OC groups among the most important actors in the field of phishing (McCafferty 2004). This perception is also shared by the Aite Group located in Boston, detecting in 2009 that the majority of data corruption originated from OC groups (Fitzgerald 2009). Also, the Federal Office for Information Security (BSI) warns that many of the highly professional and target-oriented IT attacks on private citizens, enterprises and authorities derive from organised crime and intelligence services (BSI 2011: 6).

Their participation in cybercrime enables OC groups to discover new areas of operation, but also to optimise their *modus operandi*. Simultaneously, the use of ICT and the entry into cybercrime affect the internal organisation of OC groups, which adapt to new ways of committing crimes. In 2004, the Council of Europe called for attention to the fact that cybercrime could affect the structure of OC groups. The report shows that the traditional hierarchical structure of certain OC groups prevents them from entering some cybercrime fields owing to the immanent characteristics of cybercrime.

‘Cybercrime requires less control over a geographical territory, less violence and intimidation, less personal contacts and thus less relationships based on trust and enforcement of discipline between criminals.’ (Council of Europe 2004: 124)

Accordingly, different OC groups, depending on their organisational structure, would benefit in different ways from cybercrime (Council of Europe 2004: 124).

Europol, too, states that the internet can change the structure of OC groups so that hierarchical structures give way to forms supporting the specific skills of individual members (Europol 2011: 6).

7 Conclusion

The review of literature, which has gathered central statements from relevant sources, shows that the empirical research upon the phenomenon of cybercrime in general, as well as upon its connection to OC in particular, is still in its early stages. Hence, many questions regarding forms of organisation, modus operandi, motivation and damage cannot be satisfyingly answered.

All publications with regard to cybercrime and organised crime confirm that the latest technical developments are being pursued and established by criminals. 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, as well as criminals who exclusively operate in the virtual environment, can profit amongst other things from an improved cost and time efficiency as well as from a lower detection risk.

Although the literature provides statements about the age, individual background, technical know-how, and willingness to cooperate with other cybercriminals, these assumptions are rarely based on empirical findings. The review moreover lists various typologies of cybercrime. Their division is oriented amongst other things towards the stages of development of cybercrime, the use of computer technology or the use of the internet. Just as one cannot refer to ‘the cybercrime’ for the standard criminal offence, neither can academic literature define ‘the cybercriminal’. This chapter has therefore made a distinction between the individual qualities, motivation and proceedings of cybercriminals.

In academic literature, a variety of different and partly opposed points of view on the organisational structure of cybercriminals can be found. Whereas some authors suggest that cybercriminals rather operate alone than in groups, other authors state that there exist long-lasting, job-sharing organised crime

groups in cyberspace, too. These structures in cybercrime are either ‘cyber-born’ or consist of (OC) groups that were already operating in the offline field and, moreover, enter cybercrime by making use of services (Crime-as-a-Service) or by ‘familiarising’ themselves with technically sophisticated cybercrime.

To summarise, it is no longer necessary to ask whether cybercrime is committed in an organised way, whether traditional OC groups are finding their way into cybercrime and whether this development can be held back. It is rather a question of how to keep pace with the growing professionalisation of organised criminal offenders in cyberspace.

8 References

- Ablon, Lillian / Libicki, Martin C. / Golay, Andrea A. 2014: Markets for Cybercrime Tools and Stolen Data. Hackers’ Bazaar, RAND Corporation research report, http://www.rand.org/pubs/research_reports/RR610.html (accessed 01. 04. 2015).
- Arquilla, John / Ronfeldt, David 1997: In Athena’s Camp – Preparing for Conflict in the Information Age, Santa Monica: RAND Corporation.
- Benda, Richard 2011: Die Triangel des Bösen, in: CD Sicherheits-Management Nr. 2/2011.
- Brenner, Susan W. 2002: Organized Cybercrime? How Cyberspace May Affect the Structure of Criminal Relationships, in: North Carolina Journal of Law & Technology, Vol. 4, No. 1, pp. 1–50.
- Broadhurst, Roderic / Grabosky, Peter / Alazab, Mamoun / Bouhours, Brigitte / Chon, Steve / Da, Chen 2013: Crime in Cyberspace: Offenders and the Role of Organized Crime Groups. Working Paper 15. 05. 2013, in: Australian National University Cybercrime Observatory.
- Broadhurst, Roderic / Grabosky, Peter / Alazab, Mamoun / Chon, Steve 2014: Organizations and Cyber crime: An Analysis of the Nature of Groups engaged in Cyber Crime, in: International Journal of Cyber Criminology, Vol. 8 Issue 1 January, pp. 1–20.
- Bundesamt für Sicherheit in der Informationstechnik 2011: Die Lage der IT-Sicherheit in Deutschland 2011, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte-/Lagebericht2011_nbf.pdf;jsessionid=09CA0CB66C21016CB3CAE0C824C00A6F2_cid359?__blob=publicationFile (accessed 31. 03. 2015).
- Bundesamt für Sicherheit in der Informationstechnik (eds.) 2014: Die Lage der IT-Sicherheit in Deutschland 2014, <https://www.bsi.bund.de/DE/Publikationen/Lageberichte/bsi-lageberichte.html> (accessed 08. 04. 2015).

- Bundeskriminalamt 2015: Täter im Bereich Cybercrime – Eine Literaturanalyse, http://www.bka.de/nn_205960/SharedDocs/Downloads/DE/Publikationen/Publikationsreihen/SonstigeVeroeffentlichungen-/2015Taeter-ImBereichCybercrime,templateId=raw,property=publicationFile.pdf/2015TaeterImBereichCybercrime.pdf (accessed 25. 05. 2016).
- Chiesa, Raoul / Ducci, Stefania / Ciappi, Silvio 2009: Profiling hackers. The science of criminal profiling as applied to the world of hacking, Boca Raton: CRC Press.
- Choo, Kim-Kwang R. / Grabosky, Peter 2014: Cybercrime, in: Paoli, Letizia (eds.): The Oxford Handbook of Organized Crime, New York: Oxford University Press, pp. 482–499.
- Choo, Kim-Kwang R. / Smith, Russel G. 2008: Criminal Exploitation of Online Systems by Organised Crime Groups, in: Asian Journal of Criminology, Vol. 3, No. 1, pp. 37–59.
- Council of Europe 2001: Convention on cybercrime, Budapest, 23.XI.2001 http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/T-CY/Default_TCY_en.asp (accessed 09. 04. 2015).
- Council of Europe 2004: Organised crime situation report 2004. Focus on the threat of Cybercrime, <http://www.coe.int/t/dghl/cooperation/-economic-crime/organisedcrime/Organised%20Crime%20Situation%20Report%202004.pdf> (accessed 31. 03. 2015).
- Cross, Michael 2008: Scene of the Cybercrime, 2nd ed., Syngress.
- Décary-Héту, David / Dupont, Benoit 2012: The social network of hackers, in: Global Crime, 13:3, pp. 160–175.
- Décary-Héту, David / Dupont, Benoit 2013: Reputation in a dark network of online criminals, in: Global Crime, <http://dx.doi.org/10.1080/17440572.2013.801015> (accessed 31. 03. 2015).
- Detica/BAE Systems 2012: Organised crime in the digital age. The real picture. Executive summary of BAE Systems Detica and the John Grieve Centre for Policing and Community Safety ‘Organised crime in the digital age’ research report, http://www.baesystemsdetica.com/uploads/resources-/ORGANISED_CRIME_IN_THE_DIGITAL_AGE_EXECUTIVE_SUMMARY_FINAL_MARCH_2012.pdf (accessed 02. 05. 2012), without page reference.
- Essers, Loek 2012: Russian cybercriminals earned \$ 4.5 billion in 2011. Russian mafia took control and professionalized online crime in 2011, researchers say, in: Computerworld, <http://www.computerworld.com/article/2503653/cybercrime-hacking/russian-cybercriminals-earned-4-5-billion-in-2011.html> (accessed 08. 04. 2015).
- Europol 2011: Threat assessment (abridged). Internet facilitated organized crime, Europol Public Information, <https://www.google.de/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CCYQF-jAA&url=https%3A%2F%2Fwww.europol.europa.eu%2Fsites%2Fde->

- fault%2Ffiles%2Fpublications%2Fiocta.pdf&ei=A4IZVf_MBIXzPK-LAgbgI&usg=AFQjCNEeLufQeEugufXPxGDwLsVC-Q8TrA&bvm=bv.89381419,d.ZWU (accessed 30. 03. 2015).
- Europol 2014: The Internet Organised Crime Threat Assessment (iOCTA), Europol Public Information, <https://www.europol.europa.eu/sites/default/files/publications/iocta-epub.epub> (accessed 30. 03. 2015).
- Fitzgerald, Michael 2009: Organized Cybercrime Revealed. The shadow economy for stolen identity and account information continues to evolve, in: CSOnline, <http://www.csonline.com/article/2124411/malware-cybercrime/organized-cybercrime-revealed.html> (accessed 30. 03. 2015).
- Glenny, Misha 2012: Darkmarket. Hur datahackarna blev den nya maffian, Norstedts Förlagsgrupp AB.
- Goldman, David 2011: The Cybercrime Economy. The cyber Mafia has already hacked you, in: CNNMoneyTech, http://money.cnn.com/2011/07/27/technology/organized_cybercrime/ (accessed 08. 04. 2015).
- Goodman, Marc D. 1997: Why the police don't care about computer crime, in: Harvard Journal of Law & Technology, Vol. 10, No. 3, pp. 465–494.
- Grabosky, Peter N. 2001: Virtual criminality. Old wine in new bottles?, in: Social & Legal Studies, Vol. 10, No. 2, pp. 243–249.
- Grabosky, Peter N. 2007: Electronic crime. Old Tappan: Pearson Education.
- Grabosky, Peter N. 2013: Organised Crime and the Internet, in: The RUSI Journal, 158:5, pp. 18–25.
- Group IB 2011: State and Trends of the 'Russian' Digital Crime Market 2011, http://www.group-ib.com/images/media/Group-IB_Report_2011_ENG.pdf (accessed 30. 03. 2015).
- Hutchings, Alice 2014: Crime from the keyboard: Organised crime, co-offending, initiation and knowledge transmission, in: Crime, Law and Social Change, Vol. 62, No. 1, pp. 1–20.
- Koops, Bert-Jaap 2010: The internet and its opportunities for cybercrime, Tilburg Law School Legal Studies Research Paper Series No. 09/2011, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1738223 (accessed 25. 03. 2015).
- Lavorgna, Anita 2013: Transit crimes in the internet age. How new online criminal opportunities affect the organization of offline transit crimes, thesis at the University of Trento, <http://eprints-phd.biblio.unitn.it/1185/> (accessed 26. 03. 2015).
- Lavorgna, Anita 2014: Internet-mediated drug trafficking: towards a better understanding of new criminal dynamics, in: Trends in Organized Crime, Vol. 17, No. 4, pp. 250–270.
- Lavorgna, Anita 2015a: Organised crime goes online. Realities and challenges, in: Journal of Money Laundering Control, Vol. 18, No. 2.

- Lavorgna, Anita 2015b: The online trade in counterfeit pharmaceuticals. New criminal opportunities, Trends and challenges, in: *European Journal of Criminology*, Vol. 12, No. 2, pp. 226–241.
- Leukfeldt, E. Rutger (2014). Cybercrime and social ties. Phishing in Amsterdam. *Trends in Organised Crime*, 17, 231–249.
- Leukfeldt, E. Rutger (2015), Organised Cybercrime and Social Opportunity Structures: a Proposal for Future Research Directions, *The European Review of Organised Crime*, 2(2), 91–103.
- Li, Xingan 2008: The Criminal Phenomenon on the Internet: Hallmarks of Criminals and Victims Revisited through Typical Cases Prosecuted, in: *University of Ottawa Law & Technology Journal*, pp. 125–140.
- Lu, ChiChao / Jen, WenYuan / Chang, Weiping / Chou, Shihchieh 2006: Cybercrime & Cybercriminals: An Overview of the Taiwan Experience, in: *Journal of Computers*, Vol. 1, No. 6, September 2006, pp. 11–18.
- Lusthaus, Jonathan 2012: Trust in the world of cybercrime, in: *Global Crime*, Vol. 13, No. 2, May 2012, pp. 71–94.
- Lusthaus, Jonathan 2013a: Electronic ghosts, in: *Democracy Journal*, No. 31/2014, pp. 45–60.
- Lusthaus, Jonathan 2013b: How organised is organised cybercrime?, in: *Global Crime* 14: 1, pp. 52–60.
- Marcum, Catherine D. / Higgins, George E. / Tewksbury, Richard 2012: Incarceration or community placement: examining the sentences of cybercriminals, in: *Criminal Justice Studies*, 25(1), pp. 33–40.
- McCafferty, Dennis 2004: Organized Cyber Crime, <http://www.thewhir.com/organized-cyber-crime> (accessed 01.04.2015), without page reference.
- McCusker, Rob 2006: Transnational organised cyber crime. Distinguishing threat from reality, in: *Crime, Law and Social Change*, Vol. 46, No. 4–5, pp. 257–273.
- McCusker, Rob 2011: Organised cybercrime: myth or reality, malignant or benign?, in: Manacorda, Stefano (ed.): *Cybercriminality: Finding a balance between freedom and security*, in: *Selected papers and contributions from the International Conference on ‘Cybercrime: Global Phenomenon and its Challenges’*, Courmayeur Mont Blanc, Italy, 2–4 December 2011, pp. 107–116.
- McGlasson, Linda 2009: Lexis-Nexis Breach Linked to Crime Family – Analyst: ‘Days of Amateurs Committing Breaches are Well Behind Us’, http://www.bankinfosecurity.com/articles.php?art_id=1632&opg=1 (accessed 08.04.2015).
- McGuire, Mike / Dowling, Samantha 2013: Cyber crime: A review of the evidence. Summary of key findings and implications, Home Office research report 75, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/246749/horr75-summary.pdf (accessed 09.04.2015).

- McMillan, Robert 2009: LexisNexis Warns of Breach After Alleged Mafia Bust, in: PCWorld, <http://www.pcworld.com/article/168311/article.html> (accessed 30. 03. 2015).
- Nisbett, Carolyn 2002: New directions in cyber-crime, in: White Paper, QinetiQ.
- Peachey, Paul 2014: Mafia cybercrime booming and with it a whole service industry, says study, in: The Independent, <http://www.independent.co.uk/news/uk/crime/mafia-cybercrime-booming-and-with-it-a-whole-service-industry-says-study-9763447.html> (accessed 08. 04. 2015).
- Poole-Robb, Stuart 2015: The Mafia moves online: Are you at risk?, in: IT-ProPortal, <http://www.itproportal.com/2015/04/21/mafia-moves-online-you-at-risk/> (accessed 08. 04. 2015).
- Protalinski, Emil 2008: Report – cybercrime groups starting to operate like the Mafia. A new report from web security company Finjan says that cybercrime has evolved, arstechnica, <http://arstechnica.com/business/2008/07/report-cybercrime-groups-starting-to-operate-like-the-mafia> (accessed 08. 04. 2015).
- Rogers, Mathew 2006: A two-dimensional circumplex approach to the development of a hacker taxonomy, in: Digital Investigation, (3), pp. 97–102.
- Sandywell, Barry 2010: On the globalisation of crime. The Internet and new criminality, in: Jewkes, Yvonne / Yar, Majid (eds.): Handbook of Internet Crime, Cullompton: Willan Publishing, pp. 38–66.
- Schönbohm, Arne 2013: Cybercrime – Lukratives Geschäft für die Organisierte Kriminalität, in: Aus Politik und Zeitgeschehen, 38–39/2013, pp. 28–34.
- Schönbohm, Arne 2014: Organisierte Kriminalität goes digital, [http://www.securityexplorer.de/index.php?id=20&tx_ttnews\[tt_news\]=170&cHash=329d80f946059c7128a88efc59305de9](http://www.securityexplorer.de/index.php?id=20&tx_ttnews[tt_news]=170&cHash=329d80f946059c7128a88efc59305de9) (accessed 08. 04. 2015).
- Symantec Corporation 2010: The Norton Cybercrime Report. The Human Impact, http://us.norton.com/content/en/us/home_homeoffice/media/pdf/-cybercrime_report/Norton_USA-Human%20Impact-A4_Aug4-2.pdf (accessed 08. 04. 2015).
- Tapscott, Don / Williams, Anthony D. 2007: Wikinomics: How mass collaboration changes everything, London: Atlantic Books.
- The Swedish National Council for Crime Prevention (Brottsförebyggande rådet, Brå) (eds.) 2000: IT relaterad brottslighet (IT-related criminality).
- The WHIR 2004: Mafia Adult Hosting Operation Indicted, <http://www.the-whir.com/web-hosting-news/mafia-adult-hosting-operation-indicted> (accessed 08. 04. 2015).
- Thomas, Douglas / Loader, Brian D. 2000: Cybercrime in the information age, in: Thomas, Douglas / Loader, Brian D. (eds.): Cybercrime: Law Enforcement, Security and Surveillance in the Information Age, Routledge, pp. 6–7.

- Tropina, Tatiana 2010: Cyber Crime and Organised Crime, UNICRI, <http://f3magazine.unicri.it/?p=310> (accessed 08. 04. 2015).
- Tropina, Tatiana 2012: The evolving structure of online criminality. How cybercrime is getting organized, in: *Eucrim* 4/2012, pp. 158–165.
- UNICRI/Chiesa, R. 2009: Profiling Hackers, http://www.unicri.it/special_topics/securing_cyberspace/-current^nd_past^ctivities/hackers_profiling/ (accessed 08. 04. 2015).
- UNODC 2010: The Globalization of Crime. A transnational organized crime threat assessment, https://www.unodc.org/documents/data-and-analysis/tocta/TOCTA_Report_2010_low_res.pdf (accessed 08. 04. 2015).
- UNODC 2012: Digest of Organized Crime Cases. A compilation of cases with commentaries and lessons learned, https://www.unodc.org/documents/organized-crime-/EnglishDigest_Final301012_30102012.pdf (accessed 08. 04. 2015).
- UNODC 2013: Comprehensive Study on Cybercrime, https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf (accessed 08. 04. 2015).
- Wall, David S. 2007: The transformation of crime in the information age, Cambridge: Polity Press.
- Wall, David 2010a: Criminalising cyberspace. The rise of the internet as a ‘crime problem’, in: Jewkes, Yvonne / Yar, Majid (eds.): *Handbook of internet crime*, pp. 88–103.
- Wall, David 2010b: The organization of cybercrime and organized cybercrime, in: Bellini, Marcello / Brunst, Phillip / Jähnke, Jochen (eds.): *Current Issues in IT Security. Proceedings of the interdisciplinary conference in Freiburg i. Br., Germany, May 12–14, 2009*, Berlin: Dunker & Humblot.
- Wall, David 2014: Internet mafias? The dis-organisation of crime on the internet, in: Caneppele, Stefano / Calderoni, Francesco (eds.): *Organized Crime, Corruption and Crime Prevention. Essays in Honor of Ernesto U. Savona*, Heidelberg, New York, Dordrecht, London: Springer.

Worldwide the digitalisation of society is proceeding rapidly, while influencing almost all areas of life. Especially because of trends like the growing number of networked devices (the 'internet of things'), citizens' and societies' dependence on the internet will continue to grow. Since law-abiding society continuously interacts with digital-based devices and tools that are often connected to the internet, it would be naive to think that the criminal world would act differently.

The central criminological research institutes of Germany, the Netherlands and Sweden – the Criminalistic Institute of the Federal Criminal Police Office (BKA), the Research and Documentation Centre (WODC) of the Dutch Ministry of Security and Justice and the Swedish National Council for Crime Prevention (Brå) – conducted extensive empirical research to enlighten the links and convergence between cybercrime and organised crime.

The project "Cyber-OC – Scope and manifestations in selected EU member states" was funded by the European Union Programme 'Prevention of and Fight against Crime (ISEC)' for the duration of two years (from April 2014 to March 2016). This book contains the case studies of the three project partners, a common concluding chapter as well as an extensive literature review. This volume provides essential insights and police-relevant findings concerning the crime phenomenon of Cyber-OC.