EMPACT – OAP Cyber-Attacks

OA 8.1 ‘Cybercrime and organised crime / Organised cybercrime’

Literature Review Report

Criminal Structures on Illegal Online Platforms

Karsten Kasper

in collaboration with

Gergana Bulanova-Hristova

(February 2017)
Funded by the European Union as part of the Europol EMPACT priority “Cyber Attacks”. This report reflects the views only of the authors. The European Commission cannot be held responsible for any use which may be made of the information contained therein.
## Contents

Figures ..................................................................................................................................................... 4
Abstract ................................................................................................................................................... 5

1. Background ........................................................................................................................................... 6
2. Introduction to the subject .................................................................................................................. 6
3. Research questions, approach and definitions .................................................................................... 8
   3.1. Research questions ...................................................................................................................... 8
   3.2. Methodology ............................................................................................................................. 8
   3.3. Definitions .................................................................................................................................. 9
4. Illegal online platforms – possibilities and limitations for scientific research ....................................... 10
   4.1. Data collection methods ............................................................................................................. 10
      4.1.1. Secondary data .................................................................................................................... 10
      4.1.2. Primary data ......................................................................................................................... 11
   4.2. Data analysis methods ................................................................................................................. 14
      4.2.1. Social network analysis ....................................................................................................... 14
      4.2.2. Crime Script Analysis .......................................................................................................... 17
      4.2.3. Grounded Theory ............................................................................................................... 17
      4.2.4. Social Opportunity Structure Perspective and Routine Activity Theory .......................... 19
      4.2.5. Theory-independent evaluations ....................................................................................... 19
5. The online black market – an overview .................................................................................................. 21
6. Illegal online platforms structuring criminal activities ......................................................................... 23
   6.1. Protagonists and their tasks within the platform-internal hierarchy ............................................ 23
   6.2. Reputation systems .................................................................................................................... 27
   6.3. Fiduciary systems ...................................................................................................................... 29
   6.4. Quality control .......................................................................................................................... 29
   6.5. Digital contracts ........................................................................................................................ 30
7. Online groups on illegal online platforms ............................................................................................ 31
8. Offline groups on illegal online platforms .......................................................................................... 33
   8.1. Number of OC groups active on online platforms ...................................................................... 35
   8.2. Effects of OC involvement in illegal online platforms ............................................................... 35
9. Challenges and recommendations for action ........................................................................................ 39
   9.1. Potential courses of action for law enforcement authorities ...................................................... 39
      9.1.1. Increasing the effort to commit the crime .............................................................................. 39
      9.1.2. Increasing the risks of committing the crime ...................................................................... 42
      9.1.3. Reducing the rewards of committing the crime ................................................................. 42
      9.1.4. Reducing incentives and removing any excuses ............................................................... 43
   9.2. Positioning of the law enforcement authorities .......................................................................... 44
   9.3. National and international cooperation ....................................................................................... 45
   9.4. New developments ..................................................................................................................... 47
10. Conclusion and need for action .......................................................................................................... 48
11. References ........................................................................................................................................ 50
Figures

Figure 1: Centralised and decentralised organisational structure ......................................................... 14
Figure 2: Graphic representation of the investigated network ............................................................... 15
Figure 3: Connections between hacker groups ..................................................................................... 16
Figure 4: Characteristics of different forms of social organisation of criminals ................................. 18
Figure 5: Typical hierarchy of a carding forum .................................................................................... 25
Figure 6: Levels within an underground marketplace ........................................................................ 26
Figure 7: Illustration of the regulatory system of carding forums ..................................................... 31
Figure 8: Groups of perpetrators formed on online platforms ............................................................ 32
Abstract

This report presents the findings of a literature review on the subject of “criminal structures on illegal online platforms”. Among other things, the analysis focused on the following questions: What is the structure of illicit online platforms? Do they contribute to the formation of new criminal groups, and if so, how? How are they being used by Organised Crime (OC) groups?

The following key findings can be derived from the literature review:

- Illegal online platforms have already been subjected to scientific analysis many times, using a variety of different methods of investigation and pursuing different objectives. While many authors endeavoured to investigate the full scope of the online black market, others focused on specific aspects such as the products and services being offered, the earnings achieved by the users, the protagonists (background, motivation, etc.), the money flows, the mechanisms used for encryption and for generating trust. In a small number of the sources, the relationships and the criminal cooperation between the members of a platform represented the central subject matter of investigation.

- On the one hand, illegal online platforms with their inherent mechanisms, rules and social processes are seen as a type of criminal structure by some authors (Chapter 6).

- On the other hand, the concept of criminal structures also refers to the criminal cooperation between members of a platform within different forms of cooperation – e.g., networks featuring a division of labour, hierarchical groupings of perpetrators, or even OC groups – (Chapters 7 and 8). Other authors accordingly focused on the investigation of groups of perpetrators appearing on these platforms. In this context, the platforms themselves merely represent a type of sphere of activity for these groups.

- Going by the specialist literature, there can be little doubt that groups of (traditional) Organised Crime are active on online platforms, yet there is little empirical research on this particular subject (Chapter 8). OC groups make use of online platforms for, among other things, the trade with illegal goods and the recruitment of accomplices.

- About half of the sources evaluated provided recommendations for action for cybercrime investigations in the area of illegal online platforms (Chapter 9). They cover measures relating to investigative measures, the positioning of the law enforcement authorities in terms of organisation and content, and their cooperation with different protagonists.

- Since the utilisation of illegal online platforms by groups of perpetrators formed offline and online has never been the central subject of an empirical assessment based on primary data to date, more research will be needed in this area. Given that cybercrime is an international phenomenon and that the sphere of influence exerted by groups of Organised Crime is also on an international scale, a study with an international scope would clearly benefit law enforcement.

1 The general term “online platform” covers both forums and marketplaces.
1. Background

This literature review was carried out as part of the EMPACT action OA 8.1 “Cybercrime and Organised Crime / Organised Cybercrime” conducted between April and December 2016 with the aim of surveying and analysing the current state of research on the subject of “criminal structures on illegal online platforms”. The report is addressed at both the European law enforcement authorities and an interested specialist audience in the field of security research.

2. Introduction to the subject

Transnational groups of Organised Crime are inventive when it comes to boosting their profits, and so they have been aware for some time that getting involved in cybercrime is worthwhile. Increasing use of the Internet in all areas of life and worldwide networking have led to a heightened danger for ordinary citizens as well as for business, public administration and political circles to become victims of Organised (cyber) Crime (cf. UNODC 2016 and INTERPOL 2016). Not only the entry into cybercrime by Organised Crime itself is considered dangerous, but also the fact that cybercrime groups are being formed which commit cybercrime over extended periods of time by working in a highly professional, collaborative and profit-oriented manner.

Illegal Internet forums and marketplaces in the clearnet as well as the darknet are speeding up these developments in that they facilitate and promote the commission of cybercrime in collaboration with others. They are frequently characterised by complex structures, specialised roles and extensive division of labour (cf. Ablon et al. 2014: ix). They structure cybercriminal activities, lead to the formation of new types of “cyberborn groups” and they are utilised profitably by Organised Crime groups (cf. Bulanova-Hristova et al. 2016: 36, 111 and 181). Their hierarchical structure simplifies criminal cooperative ventures, allows information, goods, data and services to be exchanged, and helps individual criminals or groups identify supporters and recruit new members. With their anonymisation mechanisms and their international nature, illegal online platforms also present law enforcement authorities with new challenges. An added factor is that their use does not require sophisticated technical skills, and they therefore attract many new Internet users – such as customers interested in illegal products and services on the one hand, and sellers (incl. groups based in traditional Organised Crime) who recognise the potential of a global, anonymised and violence-free market on the other (cf. Lewman 2016: 36). The relative ease of use of these online platforms greatly facilitates initial involvement in cybercrimes, enabling users without sound technical skills to commit sophisticated cybercriminal activities by making use of toolkits and customer services (incl. call centres) (cf. Merces 2014: 1).

Similar to the World Wide Web, illegal forums and marketplaces exist in a realm without boundaries and can be accessed from anywhere in the world. In addition to an international, English-language

---

online black market\(^3\), there are successful regional variants, e.g., for the Russian, Chinese or Brazilian market (cf. Merces 2014: 1). Online forums and marketplaces have been in existence since as far back as the early 2000s. One of the first such forums was the Russian “carderplanet.com”, which operated in the clearnet. The “ShadowCrew” forum, where hacked, stolen and falsified data (credit cards, passports, birth certificates, etc.) were traded along with hacking/cybercrime tools, was hosted in Hong Kong, and as early as the year 2002 it already had around 2,500 members in about seven countries (cf. Buxton/Bingham 2015: 4).

Illegal online platforms are often located in the darknet. Trading with narcotics in particular often takes place on the clearnet as well, however. The first black markets for narcotics on the darknet were created in 2009 and they were able to operate relatively unchecked, whereas their successor Silk Road was less discreet and was monitored closely not only by law enforcement authorities, but also by the public (cf. van Slobbe 2016: 77).

Online platforms for cybercrime tools (“exploit kits”\(^4\), bots\(^5\) for DDoS attacks\(^6\), ransomware\(^7\), malware\(^8\)), cybercrime services and stolen data have a major threat potential since they can be used in the preparation and execution of dangerous attacks on Internet users, businesses, administrative bodies, political figures and others. Moreover, they provide an infrastructure for selling vast amounts of stolen data and sensitive information. According to the specialist literature, platforms for cybercrime tools can in some cases generate higher criminal earnings than the illegal trade with narcotics (cf. Ablon et al. 2014: ix).

This report is structured as follows: In a first step, the methodology underlying the literature review is described in more detail, and relevant terminology is explained (Chapter 3). This is followed by a description of the data collection and analysis methods that have been employed in the investigation of illegal online platforms to date (Chapter 4). Chapter 5 is a brief overview of the illegal online black market. This is followed by an explanation as to how illegal online platforms themselves can be considered criminal organisations on the basis of their hierarchical structure, the existing division of labour and their complex regulatory mechanisms (Chapter 6). In addition, illegal online platforms also lead to the formation of independent online groups of perpetrators who make use of them for different kinds of interaction (Chapter 7). The next chapter contains findings in relation to the utilisation of illegal online platforms by offline Organised Crime groups (Chapter 8). This is followed by a presentation of the challenges posed to law enforcement authorities discussed in the specialist literature, as well as the recommendations for action identified therein (Chapter 9). The report ends with a brief conclusion and the recommendations for action identified (Chapter 10).

\(^3\) The term online black market is used in the following to refer to criminal online platforms in their entirety.

\(^4\) A toolkit that can be used to disseminate malicious software through web-based attacks. “A typical exploit kit usually contains a management console, a number of vulnerabilities of various applications, and several add-on functions that help cybercriminals to launch a broad-based attack” (Chen/Li 2015: 3).

\(^5\) A malware program capable of executing tasks independently and automatically (cf. BSI 2016).

\(^6\) “An attack on a computer with the aim of eliminating its availability. The attack is launched from a great number of distributed computers” (BKA 2016c).

\(^7\) “Ransomware refers to a certain type of trojan/malware designed to encrypt a user’s data in such a way that the user will only be able to re-gain access to his data after paying a ransom. Alternative names for ransomware are blackmail trojans [...] and encryption trojans” (eco 2016).

\(^8\) “Malware stands for ‘malicious software’. It is written with the aim of infiltrating a computer system [...] without the owner’s permission in order to gain control over the device, steal valuable information or corrupt data” (BKA 2016d).
3. Research questions, approach and definitions

3.1. Research questions

The evaluation of the specialist literature showed that illegal online platforms have been the subject of several different studies in the past – for example, the online platforms themselves were investigated with regard to, among other aspects, their structure and mechanisms, the products and services offered, and the origin and motivation of their members. However, the links between online platforms and organised commission of cybercrime, or between the platforms and Organised Crime, have only been studied in passing, if at all. There have been relatively few empirical investigations relating to the role of online platforms in the emergence of new criminal structures in particular, or to the platforms’ utilisation by protagonists of Organised Crime. Initial empirical findings on these particular aspects were produced in the context of the international “Cyber-OC – Scope and manifestations in selected EU member states” project. These findings show that, among other things, illegal online platforms facilitate and structure criminal cooperation between cybercriminals, enable the formation of new cybercriminal groupings, and that the platforms are actively being utilised by “established” Cyber-OC groups (cf. Bulanova-Hristova et al. 2016: 181 ff.).

Based on the findings of the “Cyber-OC” project, this report was written with a particular focus on the investigation of organised cybercrime on illegal online platforms. The main question was how criminal structures are represented on illegal online platforms in the clearnet and the darknet. More specifically, the analysis focused on how illegal online platforms are structured, what structures and mechanisms they employ to facilitate exchanges and cooperation between cybercriminals, how they contribute to the formation of new groups, and how they are exploited by Organised Crime groups.

3.2. Methodology

In preparing this report, an evaluation was made of publicly available sources investigating collaboratively committed cybercrimes in general and/or those more specifically studying the relationship between cybercrime and online platforms in the clearnet and the darknet.

In terms of content, this literature review builds on the findings of the literature review carried out as part of the “Cyber-OC” project (cf. Dietrich et al. 2016). This means that several thematically relevant sources that had been identified during the preceding evaluation by means of systematic keyword-based searches were already known and could be included in this report. Additional texts were identified via the so-called snowball method, which refers to the identification of texts with potential relevance for the present evaluation via the bibliographies contained in sources that are already known. Sources considered particularly relevant in terms of the subject matter where those focusing on the organised commission of cybercrimes and the utilisation of online platforms in the darknet and clearnet – e.g., referencing to protagonists and/or structures of online platforms – or in which thematically relevant primary data was collected and analysed, since these provide examples of potential research methodologies with their respective advantages and shortcomings. However, the evaluation also included sources where this subject was only dealt with in passing.

---

9 Searches of online library catalogues, specialised databases and websites of relevant institutions using a set of defined search terms.
The literature search produced a large number of hits. An initial review of the sources showed that the vast majority made no reference to groups of perpetrators on online platforms, and they were therefore not included in the subsequent evaluation. A total of 40 sources (papers reporting the findings of research projects and studies, doctoral and diploma theses, scientific articles and police reports) in English and German and published between 2007 and 2016 were included. The literature was summarised using a matrix and evaluated in terms of content using the following criteria: Research questions and research subject; methodology; findings relating to the organisational structure of online platforms, interaction between different protagonists, utilisation by OC groups; recommendations for action addressed to law enforcement authorities.

3.3. Definitions

The Internet is commonly perceived as consisting of three separate realms. The clearnet (also referred to as the surface web) comprises freely accessible content that can be found using search engines. In contrast, on the deep web content cannot be accessed via search engines as it is protected by passwords, for example. The darknet, in turn, is part of the deep web, a part of the Internet that can only be accessed using special anonymisation services such as the Tor browser, and where IP data and communications are anonymised (cf. BKA 2016a: 1).

In the opinion of police and scientists, the cybercrime phenomenon can be understood in both a narrow and a broad sense. In this view, cybercrime on the one hand comprises “actions where the Internet, data networks, information technology systems or their data are the target of criminal conduct” (cybercrime in a narrow sense) and on the other, crimes “where this information technology is used as a means” (cybercrime in a broad sense) (BKA 2013b: 5). In cybercrime in the broad sense, the Internet is frequently used in the planning, preparation and execution of a criminal act. Accordingly, the illegal narcotics trade via online platforms is also considered to be cybercrime in the broad sense (cf. Van Slobbe 2016: 77).

The specialist literature distinguishes between forums and marketplaces. Whereas illegal forums primarily allow cybercriminals to exchange information, communicate and transfer data, the marketplaces specialise in the illegal trade with, among other things, goods, services, data and technical expertise (cf. BKA 2016a: 2). The marketplaces are characterised by regulated technical procedures (e.g., for payments), which speeds up transactions. To a lesser extent trading is also carried out on forums, but there it is not automated and therefore more time-consuming. However, according to Trend Micro trade in selected goods is still frequently conducted on forums as they offer greater flexibility than the marketplaces when it comes to negotiating changes and special terms and conditions (cf. Trend Micro 2015: 24). Wherever the terms forum and marketplace are used synonymously in the literature, or where definitions of terms were not provided, this reports uses the more general term "online platform", which covers both forums and marketplaces. The term cryptomarket is used to describe marketplaces that are situated in the darknet and can therefore only be used through anonymising services (cf. Lewman 2016: 36).
4. Illegal online platforms – possibilities and limitations for scientific research

Online platforms in the clearnet and the darknet have been analysed many times and with different objectives. While many authors attempted to investigate the online black market as fully as possible, others focused on specific aspects. Since these studies employed a multitude of different research methodologies, the data generated through these analyses also differs. The next section begins by describing the data collection methods identified in the evaluated sources (4.1). This is followed by a summary of the approaches taken in evaluating the collected primary and secondary data. The theories and objectives underlying the evaluations, the results relevant to the literature evaluation, as well as the weaknesses and limitations of the applied methods are then discussed (4.2).

4.1. Data collection methods

4.1.1. Secondary data

Several of the sources evaluated are based on the evaluation of freely accessible sources (incl. newspaper articles, scientific studies, journal articles). While the scientific significance of evaluations based on existing rather than independently collected data (so-called secondary data) is limited, it can be enhanced through the inclusion of a large number of sources that are as diverse in nature as possible (cf. Carley 2007: 1335). For example, for their 2010 study Lu et al. (2010) extracted "concepts" (thematically relevant ideas) from publicly accessible sources such as newspaper articles and papers published in scientific journals which they then evaluated as part of a social network analysis (cf. Lu et al. 2010: 35). They stated that while the information density of this data was meaningful, it did not contain as much information as police investigation files or the backups of interactions that had occurred on online platforms (communications, sales, purchases, feedback, etc.). The authors therefore recommended that additional evaluations be carried out, for example of the backed up contents of platforms (so-called "dumps") in order to gain more detailed findings (cf. Lu et al. 2010: 40).

In an effort to find out why cybercriminals engage in extensive cooperative ventures on the Internet despite the anonymity and the attendant absence of trust, Lusthaus (2012) evaluated the archived media statements from the US Ministry of Justice on judicial proceedings in the area of cybercrime. Lusthaus also evaluated a variety of other texts, such as reports from private security personnel and newspaper articles (cf. Lusthaus 2012: 75 f.). A different approach was taken by Broadhurst et al. (2014). They compared and evaluated the results of two studies dealing with links between Organised Crime and cybercrime which also contained typologies of perpetrators. Broadhurst et al. used several recent cybercrime cases that had been reported in the media in order to test the meaningfulness of the perpetrator typologies provided (cf. Broadhurst et al. 2014: 2).

Added to this are journal articles based on literature reviews which, among other things, deal with subjects such as reputation on cryptomarkets (cf. Cox 2016), the gaps in the scientific research into illegal online markets (cf. Holt 2016), the methods and strategies for investigating online markets for stolen data (cf. Hutchings/Holt 2016), the cryptomarket as a new criminological concept (cf. Martin 2014), or the use of cryptomarkets for the narcotics trade (cf. Van Slobbe 2016).
4.1.2. Primary data

One popular and widely used method for collecting primary data is conducting interviews with experts. Lusthaus (2012), for example, in an effort to gain insight into the subject of "trust in cybercrime", and in addition to analysing publicly available texts, conducted several interviews with members of law enforcement authorities and staff of private cybersecurity companies as well as with hackers (cf. Lusthaus 2012: 75 f.). Van Hout and Bingham (2013) asked a Silk Road user about his experiences in interacting with other members, among other things. Ablon et al. (2014) interviewed more than 20 experts and supplemented their study with an evaluation of the relevant specialist literature and media articles (cf. Ablon et al. 2014: 2). Their aim was to investigate marketplaces for cybercrime tools and stolen data in order to gain a better understanding of their characteristics (structure, the way they function, their membership, products, prices) and the way they developed (cf. Ablon et al. 2014: 1 f.).

In their report “The Rise and Challenge of Dark Net Drug Markets” Buxton and Bingham (2015) describe the creation and spread of illegal online drug markets and the associated challenges for law enforcement authorities (cf. Buxton/Bingham 2015: 2). As part of their research they conducted interviews with experts and with users of the Tor network (cf. Buxton/Bingham 2015: 3). In the investigation carried out by Ormsby (2016), active Silk Road members (buyers, sellers, employees) from around the world were interviewed in person and/or in writing in order to find out more about the “typical” Silk Road user, the prices and availabilities of the products, the platform in general (quality of the products, harm reduction, ideals and values specific to sub-groups) and the approach taken by the law enforcement authorities in combating the platforms and their users. One limitation of the underlying data mentioned by the author is the bias resulting from the fact that many interviewees volunteered, rather than being chosen randomly by the author (cf. Ormsby 2016: 61).

Furthermore, data collection is also possible via written and face-to-face consultations or via contributions made during workshops or round table discussions. As with most of the other investigations, such surveys are frequently supplemented with a literature review – as was the case, for example, in the context of the National Strategic Assessment of Serious and Organised Crime 2016 by the National Crime Agency (NCA 2016) or the Internet Organised Crime Threat Assessment reports published annually by Europol (2016, 2015, 2014).

In many articles analysed, the authors had access to interactional or user data stored directly on illegal online platforms. Holt et al. (2012) analysed the structure of several Russian-language groups of hackers and malware programmers by collecting and evaluating the data pertaining to 336 members of a social network. The individual user profiles provided them with information about their relationships with other users, their interests, attitudes, origin and their user behaviour (cf. Holt et al. 2012: 894).

Yip et al. (2012) had access to the anonymised text message protocols from four Internet forums on which credit card data and associated services were traded. Their investigation was aimed at developing an approach for gaining a better understanding of the workings of the so-called underground economy, and ultimately also of Organised Crime, by analysing the social dynamics and the relationships between the members of these forums (cf. Yip et al. 2012: 60). In their subsequent study, Yip et al. (2013) looked at the reasons why Internet forums, despite being infiltrated and shut down by law enforcement authorities on a regular basis, continue to be used for the online trade in
stolen data. The data used in their evaluation consisted of anonymised interactional data – incl. private messages between members of well-known carding forums (cardersmarket and darkmarket) – as well as qualitative data from the backed-up archive of the “Shadowcrew” forum (cf. Yip et al. 2013: 2). The authors pointed out that private messages represent the most intimate form of exchange between forum members and can therefore provide the most detailed information about their relationships (cf. Yip et al. 2013: 6).

*Motoyama et al. (2011)* were able to access the complete backup of the activities of the members of six illegal Internet forums. Each of these forums contained large amounts of information, including members’ registration data, private messages between the members, posting in forum discussions, the member status, and a list of members who had been blocked. The platforms that were analysed offered trade in malware and other cybercrime tools or credit card data, among other things. Over 2.5 million forum postings, 900,000 private messages and 100,000 users were included in the analysis (cf. Motoyama 2011: 2). For their analysis, *Hutchings and Holt (2014)* accessed around 1,900 postings to discussions from sellers and buyers on 13 online forums dealing with stolen data (cf. Hutchings/Holt 2014: 4). In order to test whether social network analysis is a suitable method for collecting information about cybercriminals and hence would be of benefit to law enforcement authorities as well, *Decary-Hetu and Dupont (2012)* evaluated about 4,700 online conversations taken from investigations into a hacker group conducted by the Canadian police (cf. Decary-Hetu/Dupont 2012: 4). The authors built a database recording the nicknames of both partners in a conversation, the initiator, the duration as well as the contents of the conversations. Based on their evaluations, the authors succeeded in identifying 771 users (cf. Decary-Hetu/Dupont 2012:5).

In his 2012 study, *Holt* investigated the social dynamics within Russian-language online markets by subjecting the relationships between buyers and selling to a detailed analysis. To this end, he saved all freely accessible postings in discussions held on ten Russian-language forums with a total of 1,300 members. His random sample comprised just over 4,000 postings (cf. Holt 2012: 4). *Holt (2013)* also analysed the structures of closed online platforms hosting the trade in stolen online banking data. To develop a detailed descriptions of the administrative structures, the allocation of roles and the relationships between sellers, buyers and administrators and moderators of the online platforms (cf. Holt 2013: 155), he evaluated a random sample of around 200 discussions (so-called “threads”) from four online platforms with a total of around 550 users. The threads comprised more than 1,100 separate postings (cf. Holt 2013: 158 ff.).

For quantitative evaluations in particular, where the focus was on types of products, earnings and quantities sold, etc., many authors relied on so-called *spiders or crawlers*. These are software programs used to index and copy data from online platforms in their entirety – all members, postings in threads, products, ratings, etc. – or selectively – targeting only on specific members or product ranges. This approach was frequently chosen with the aim of describing the entire structure of one or more online platforms, in other words, the ecosystem of the online black market. In the *Intelliagg report* “Deeplight – Shining a light on the Dark Web”, for example, Tor web pages were indexed using the “Darksum” software program and then evaluated in relation to the languages used, the products and services offered for sale, as well as other aspects (cf. Intelliagg 2016: 6). For its report “Shedding light on the dark web”, *The Economist* accessed primary data which “Gwern Branwen” had copied from about 90 cryptomarkets between December 2013 and July 2015 by means of a crawler and then made publicly accessible via the Dark Net Market Archives (cf. Schönleben 2015). As part of its
study, The Economist evaluated approx. 360,000 sales transactions conducted on Agora, Evolution and Silk Road 2, among others, by analysing the costs, the products sold, the country of dispatch and the merchants (cf. The Economist 2016).

**Aldridge and Decary-Hetu (2014)** also collected their primary data using a crawler which allowed them to save all product offers for narcotics – a total of 12,000 listings – and more than 1,000 seller profiles on the online platform Silk Road in September 2013 (cf. Aldridge/Decary-Hetu 2014: 7). Their analysis was intended to test the hypothesis stating that narcotics sales conducted on Silk Road went mainly to intermediaries/brokers, and much less frequently to private individuals (cf. Aldridge/Decary-Hetu 2014: 5). In their 2015 study, Soska and Christin analysed the development of the anonymous online markets over time. To this end, they collected primary data from 35 different anonymous marketplaces using a crawler. The 35 platforms were scraped (i.e. copied) a total of around 2,000 times, with between 27 and about 330,000 pages of a platform obtained in each pass. The evaluation yielded insights into volumes sold, product categories and sellers (cf. Soska/Christin 2015: 35). In a study by Kruithof et al. published in 2016, the authors used a large variety of different primary and secondary data: in addition to a literature review, they conducted interviews with experts, including representatives of law enforcement authorities, collected interactional data from eight of the biggest cryptomarkets using the “DATACRYPTO” crawler in January 2016, and evaluated police investigations (cf. Kruithof et al. 2016: 5 f.). Based on this information, the authors formulated statements regarding the volume of the online trade in narcotics and other goods and services, the number and development of illegal online platforms, the distribution routes for narcotics, the participants, and they propose options for investigation and control (cf. Kruithof et al. 2016: 2).

Primary data can also be collected by evaluating investigations. To analyse cybercriminal networks in terms of their creation, structure, modi operandi and victims, among other aspects, Leukfeldt (2016) collected and evaluated primary and secondary data (cf. Leukfeldt 2016: 3). As well as the relevant specialist literature, Leukfeldt also analysed completed police investigations from the Netherlands. In addition, he conducted interviews with several experts who had been involved in the police investigations in the Netherlands and with lead investigators in the United States, the United Kingdom and Germany, as well as with victims of cybercrime attacks. He also analysed secondary data from a database compiled by a major Dutch bank in which cases of fraud were recorded along with data obtained in interviews with victims of cybercrime (cf. Leukfeldt 2016: 3 ff.). The authors of the Cyber-OC report evaluated completed police investigations from Germany, the Netherlands and Sweden with the aim of analysing the connections and mutual influence between the cybercrime and Organised Crime phenomena. Their evaluation of the investigation files was supplemented with interviews with experts, specialist feedback from expert meetings and workshops, and an evaluation of the specialist literature (cf. Bulanova-Hristova et al. 2016: 10 ff.).

In several articles there was no specific information about the origin of the data or the methods used to collect the data. For example, the **Trend Micro** study of the Brazilian online black market only referred to constant monitoring of cybercriminal activities (cf. Merces 2014: 1). Similarly, the **Kaspersky Lab** study of Russian financial cybercrime only contained scant information in this regard. The data they used came from several investigations in which Kaspersky Lab claims to have participated in, and from monitoring the Russian-language cybercrime environment over many years (cf. Stoyanov 2015: 2). The **Trend Micro** report on Germany’s cybercriminal underground contained no information at all about the database (cf. Trend Micro 2015).
4.2. Data analysis methods

4.2.1. Social network analysis

Several authors employed social network analysis to describe the structure of a network and identify the patterns of interaction between participating protagonists. While, according to Yip et al., this approach is very well suited for providing insights into (criminal) networks and to depict them (cf. Holt et al. 2012: 897), to date it has only rarely been applied to illegal online platforms (cf. Yip et al. 2012: 60).

The secondary data collected by Lu et al. (2010) via a literature review were used to answer questions regarding the structure of a group by means of social network analysis. They distinguish between networks with a centralised or a decentralised organisational structure (cf. Fig. 1). They also point out that social network analysis methods allow sub-groups to be identified and the influence of various protagonists on the relevant network to be measured. They stress that this can provide law enforcement authorities with important starting points for their investigations (cf. Lu et al. 2010: 33) and that it can make it possible, for example, to identify members performing administrative functions or holding key positions and remove them from the network at an early stage (cf. Lu et al. 2010: 38). While organised cybercriminals acting in concert are often behind cybercrime activities, most of the research into cybercrime only focuses on individual perpetrators. Using social network analysis methods, Lu et al. were able to produce a detailed description of the structure of the hacker group they were investigating: it turned out to be a decentralised network, and they managed to collect information about the leading members and their means of exerting influence, as well as about a range of sub-groups (cf. Lu et al. 2010: 40). Since the authors only investigated a single cybercriminal group, their results are of limited validity (cf. Lu et al. 2010: 40). Moreover, explanatory and more specific information regarding the quantitative approach taken in the data evaluation was missing.

Figure 1: Centralised and decentralised organisational structure

Source: Lu et al. 2010: 34

Yip et al. (2012) also relied on social network analysis in their description of four illegal forums and the relationships between the members. In contrast to Lu et al. (2010), they were evaluating copies of the message protocols from the forums, which meant they were working with primary data (cf. Yip et al. 2012: 60). The aim of their study was to analyse the structure underlying the carding forums as well as the structural characteristics and the behavioural preferences of their members in order to make an initial contribution towards gaining a better understanding of the structure of the entire underground economy (cf. Yip et al. 2012: 60). The authors concluded that trust and reputation play an important role on carding forums, and that members who act in a trustworthy manner are able to establish relatively large networks with a large number of contacts. The outcome was that they were
able to identify members whose exclusion from the forum would be particularly effective. The authors assume that the quantitative results they produced may be of significance for the law enforcement authorities with regard to an optimised utilisation of their limited investigative resources and in the development of more effective prosecution strategies (cf. Yip et al. 2010: 60). The study does not contain self-reflection in relation to any inherent weaknesses in the underlying methodology. The absence of a qualitative evaluation, which could render the results of the quantitative evaluation of the contacts between members more substantial, can be considered a weakness.

With their 2012 study, Decary-Hetu and Dupont (2012) were aiming to find out whether social network analysis is suitable for collecting relevant information on cybercriminals within a group. More specifically, they wanted to test whether the methodology is suitable for identifying those members within a cybercriminal group who fulfil a central function within the group, and whose removal would have a serious impact on the group's continued existence (cf. Decary-Hetu/Dupont 2012: 2). To investigate the group dynamics, the authors did not look at the individual characteristics of the members of the hacker network (such as motivation); instead they analysed the structural characteristics of their interactions (cf. Decary-Hetu/Dupont 2012: 5). The analysis of the network then proceeded in two stages. In the first stage, patterns of conversation were analysed more closely – who talks to whom, who contacts whom or is contacted by whom. The intention was to identify the position of a hacker within the network and the structure of the network in general (cf. Figure 2). A range of different coefficients – "centrality, betweenness, power" – enabled them to measure the extent of mutual dependencies existing between various members (cf. Decary-Hetu/Dupont 2012: 6). In a second stage, algorithms were used to identify the most important members of a network by measuring the effects their exclusion had on the network (cf. Decary-Hetu/Dupont 2012: 7).

![Figure 2: Graphic representation of the investigated network](source: Decary-Hetu/Dupont 2012: 9)

The authors noted that social network analysis makes it possible to measure the structure of a network and the position of the central protagonists in a scientific and objective manner. Specific values indicating the effects of removing one or more members from a network provide clues as to the resources needed to destroy a network. The police resources saved in this way could then be used to monitor the network's reaction to the police measures (e.g., the arrest of a member) (cf. Decary-Hetu/Dupont 2012: 15). The authors mentioned several limitations in terms of their analysis and methodology. For example, it was not possible to capture the conversations held between all of the central protagonists. In addition, they only analysed private messages between the hackers, even
though the hackers also made use of public channels such as chatrooms (cf. Decary-Hetu/Dupont 2012: 8). Using this methodology it is possible that missing information about protagonists or their interactions can lead to distortions in the representation of the relevance of a protagonist, and thus of the entire group structure. This would lead to erroneous conclusions – for example, if insufficient information were available about the main protagonists within a group, too much attention may be paid to less important members. However, since some of the calculated values are not based on absolute numbers but on ratios, distortions could be attenuated to some extent. The authors emphasise that it is important that as many different data sources as possible are accessed for the purpose of conducting a social network analysis. They suggest that the quality of this methodology therefore depends on the quality and quantity of the data concerning the interaction between network members (cf. Decary-Hetu/Dupont 2012: 15). The information collected using social network analysis should, however, be used in conjunction with additional findings obtained from traditional police measures. In addition, carrying out a qualitative evaluation of the contents of the conversations could also lend additional depth and value to the results (cf. Decary-Hetu/Dupont 2012: 16).

Holt et al. (2012) investigated the structures of Russian-language groups of hackers and malware programmers using social network analysis methods. The aim of the study was to describe how the skills and knowledge of individual group members affect their position within the online network (cf. Holt et al. 2012: 894). The evaluation included the data of 336 hackers of a well-known Russian online network. The hackers who were active in the online network were spread over several hacker groups (cf. Figure 3). To describe the relationships between the users and the structure of the online network, the authors analysed the information contained in the user profiles, e.g., the number of comments and blog entries posted, or friendships (cf. Holt et al. 2012: 894). In addition, the authors compiled a risk index which rated the dangerousness of each user. Considered most dangerous were users who produced or sold malware and hacking tools or those acting as moderators and administrators. Around 20 per cent of users analysed belonged to the second-highest risk level, and about six per cent to the highest risk level (cf. Holt et al. 2012: 895).

The authors found that users who were active in several groups simultaneously also had the highest risk level, i.e., they were among the most dangerous hackers in the forum. The authors suggest that
as consequence, this finding highlighted the fact that the same highly specialised hackers made their services available in several network sub-groups simultaneously (cf. Holt et al. 2012: 897 f.). The study findings demonstrate that hacker groups maintain very close links, and that this allows particularly skilled users to be active in several groups simultaneously. Malware produced by them can therefore easily be used by a multitude of other, less skilled users. Hackers and malware programmers thus act with a shared collegial subculture which promotes the exchange of information and offers particular rewards for innovation and IT skills (cf. Holt et al. 2012: 902). However, the authors state that their study suffers from a number of limitations: as the data originated in only a single network, one that also covered only a limited geographical region, the findings were not representative (cf. Holt et al. 2012: 902). Furthermore, the explorative operationalisation methods developed by them might be rated differently in terms of their validity and significance by other researchers.

4.2.2. Crime Script Analysis

For a "crime script" analysis, a detailed listing and a description are drawn up of the successive steps required in the preparation, execution and completion of a crime. The purpose is to promote a complete understanding of the criminal offence, leading to the development of concrete and effective approaches for countering and preventing such crimes (cf. Hutchings/Holt 2014: 3).

Hutchings and Holt (2014) were the first to apply this method to illegal online marketplaces. They evaluated the postings in discussions held on three English-language and ten Russian-language online platforms for illegally obtained data using methods drawn from qualitative content analysis (incl. open coding) (cf. Hutchings/Holt 2014: 3). The objective was to produce a detailed exposition of the online black market for stolen data. As a result, the authors identified different phases within a criminal process: installing the required client application and drawing up of the profiles, safeguarding anonymity, selecting the best illegal online marketplace, learning specific specialist skills and the market-specific language and rules, acquiring or producing the product portfolio, promoting the products and services, quality control by the administrators, discussing the measures taken by law enforcement authorities, negotiating and communicating with other users, dispatching the products, receiving payment, transport, establishing own reputation, exchanging and laundering the illegal earnings (cf. Hutchings/Holt 2014: 5 ff.). The authors point out that this method can also be applied to other online black markets – such as weapons or narcotics. Limitations arise with regard to the generalisability of the results and the validity of the evaluated data, since the possibility exists that postings in discussion on the investigated platforms could come from covert investigators from the law enforcement authorities or from other researchers (cf. Hutchings/Holt 2014: 16).

4.2.3. Grounded Theory

To describe the group-specific values and norms that determine the relationships between members of illegal online platforms and the structure of the platforms in general, Holt (2012) relied on the “grounded theory” method and on the concept of the “normative structures”. Grounded theory is an inductive method that is claimed by the authors to be capable of investigating any kind of social phenomenon (cf. Corbin/Strauss 1990: 16). Concepts that can be derived from the underlying data (in Holt’s case they are postings in discussions) must be identified more than once. Encountering the same concept multiple times allows a comparison to be made through which the findings can be
validated (cf. Corbin/Strauss 1990: 7 f.). Normative structures are value-based rules which can be used by members of a group to guide and justify their actions (cf. Herbert 1998: 347). By applying this concept Holt was trying to identify the core values shaping the relationships between the protagonists on illegal online platforms (cf. Holt 2012: 5). Holt found that the risks associated with trading on illegal online platforms and the type of products and services offered led to the formulation of a clear set of values that shape the interactions between buyers and sellers. On the illegal online platforms he investigated, Holt identified price, customer service and trust as central, mutually linked normative structures (cf. Holt 2012: 6).

In his article published in 2013, Holt analysed the structure of online platforms on which stolen data was traded. In addition to grounded theory, he also applied the “social organisation framework” of Best/Luckenbill (1994). The questions his analysis focused on included the conditions affecting the creation and further development of forums, and the complexity of the existing division of labour (cf. Holt 2013: 161). The "social organisation framework" of Best and Luckenbill (1994) was used by Holt to review the findings he had arrived at inductively from the forum threads. Best and Luckenbill divided forms of criminal organisations based on four characteristics (cf. Figure 4), with the complexity of a criminal collaboration increasing with every additional criterion met. Belonging to a shared criminal subculture (mutual association) represents the simplest form of cooperation in this organisation model. If the second characteristic applies – joint commission of criminal offences – then a criminal cooperation reaches the next-higher level of organisational complexity. A further level of complexity occurs if the criminal cooperation involves an elaborate division of labour. If the cooperation extends over a lengthy period of time, the criminal cooperation can be referred to as a “formal organisation” (cf. Holt 2013: 157).

**Figure 4: Characteristics of different forms of social organisation of criminals**

<table>
<thead>
<tr>
<th>VARIABLE</th>
<th>Loners</th>
<th>Colleagues</th>
<th>Peers</th>
<th>Mobs</th>
<th>Formal Organizations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mutual association</td>
<td>-</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Mutual participation</td>
<td>-</td>
<td>-</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Division of labor</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Extended organization</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>+</td>
</tr>
</tbody>
</table>

Source: Best/Luckenbill 1980: 15

Holt’s analysis showed that the members of online platforms for stolen data cooperated within the framework of differing organisational levels (cf. Holt 2013: 168). Buyers and sellers interacted with each other as colleagues. At the same time, the trade can also be described as a cooperative venture between “peers”, since members recruit each other and are able to influence the actions through their recommendations. There were also differences between the platforms analysed, as two of them (both Russian-language platforms) could be called “formal organisations”, whereas other platforms would tend to be referred to as “mobs” due the short time they were in existence (cf. Holt 2013: 169). The author points out that a similar analysis should be carried out with a larger sample, so as to be able to build a sounder knowledge base (cf. Holt 2013: 169).
4.2.4. Social Opportunity Structure Perspective and Routine Activity Theory

According to Leukfeldt, the “social opportunity structure” approach originated in decades-long empirical research into Organised Crime. It postulates that temptations and opportunities on the one hand, but also cost-benefit calculations influence the decision to commit crimes on the other. Moreover, it claims that relationships with other people are a means to pursue one’s own ambitions as well as to generate social capital (cf. Leukfeldt 2016: 13 f.). By comparison, “routine activity” theory explains criminal behaviour by citing the following three factors: the perpetrator's motivation, the opportunity to commit a crime due to the presence of a suitable victim, and the absence of adequate protection (cf. Cohen/Felson 1979: 588).

In his analysis, Leukfeldt (2016) employed both these theoretical approaches. He used the "social opportunity structure" approach to investigate the origin, development and the criminal capabilities of cybercriminal networks. He applied the “routine activity” theory to describe how criminal networks choose their victims (cf. Leukfeldt 2016: 29). Leukfeldt’s study showed that, among other things, online forums perform a key role for most cybercrime groups, be it in the establishment of a cybercriminal network or in the commission of various criminal offences (cf. Leukfeldt 2016: 108 ff.). Regarding the "routine activity" theory, Leukfeldt states that the explanatory power of the approach with respect to cybercriminal networks is yet to be demonstrated satisfactorily, as many studies in which it had been applied suffered from methodological limitations. These limitations related to the database used in the studies, for example, the type of operationalisation of the “routine activity” theory, or the fact that it had only been applied to certain areas of cybercrime (cf. Leukfeldt 2016: 28 f.). Leukfeldt pointed out that, despite the use of different data collection methods, his results pertaining to cybercriminal networks cannot be generalised, as only some of the known groups had been analysed and because it was not always possible to collect all the relevant information about a network (cf. Leukfeldt 2016: 183 f.).

4.2.5. Theory-independent evaluations

In their analysis of the user activities on six online platforms, Motoyama et al. (2011) showed how these platforms are structured, how their members interact, how reputation is established and how it changes (cf. Motoyama et al. 2011: 6). They also analysed the platforms in terms of the products and services offered and investigated how the relationships between the members and the reputation of a member affected the trade and the likelihood of being excluded from the forum (cf. Motoyama et al. 2011: 4). The study does not contain a consideration regarding possible limitations inherent in the database or in the approach taken. However, the fact that the analysis included not only the number of interactions but also their quality and content meant that relatively meaningful results were produced despite the fact that the study was not based on any specific theory.

To find out why cybercriminals make frequent use of online forums as a marketplace for stolen financial data despite the fact that these regularly draw the attention of law enforcement authorities, Yip et al. (2013) analysed three well-known carding forums. The study was based on criminological, social-psychological, economic and network theories (cf. Yip et al. 2013: 2). In the final analysis, the authors identified four key socio-economic mechanisms capable of facilitating online black market trading considerably: formal controls and coordination, social networking, reduction of the uncertainty in terms of the identity of the other users, and the quality of the products and services (cf. Yip et al. 2013: 2). The authors did not themselves discuss potential limitations of their
study in terms of the methodology, the database, the analysis or the interpretation. While the statistical figures from the quantitative evaluation provide comparative values, considered on their own they would have only limited power of explanation. Additional inclusion of an analysis of the qualitative data would increase the explanatory power of the study findings considerably.

Aldridge and Decary-Hetu (2014) evaluated a variety of interactions among Silk Road users in an effort to find out whether buyers on Silk Road were intermediaries/brokers or private consumers. Feedback provided online played a particular role in this quantitative analysis. It served as an indicator for a completed sale and as the basis for the calculation of a user's annual earnings (cf. Aldridge/Decary-Hetu 2014: 9). The price demanded for the narcotics, the quantities offered and the applicable discounts, as well as the texts on the seller profiles were used as the basis for the differentiation between "retail trading" and "business-to-business sales" (brokering business) (cf. Aldridge/Decary-Hetu 2014: 10). On the basis of the calculation model constructed in this way, it was determined that depending on the type of narcotic, between 31 and 45 per cent of the earnings generated on Silk Road came from sales to intermediaries/brokers (cf. Aldridge/Decary-Hetu 2014: 12). The authors therefore concluded that the development of illegal online platforms can be interpreted as a significant criminal innovation, since it is not "only" about the sale of tiniest quantities to end users, but represented in fact a relocation of Organised Crime into cyberspace (cf. Aldridge/Decary-Hetu 2014: 16). This study, too, does not contain self-reflection in terms of the methodological limitations. Moreover, its calculation model, based as it is on subjective premises, might be considered to be of only limited explanatory power by other researchers.

Soska and Christin (2015) studied the development of anonymous online markets by means of a broad-based quantitative analysis. They investigated the development of the anonymous online black market in general, the types of products offered for sale, the impact of measures directed against the markets (e.g., intervention by law enforcement authorities), the distribution of the sellers across the various markets, and the development of protective mechanisms of the members (cf. Soska/Christin 2015: 33). The project findings showed that the earnings achieved on illegal online markets ranged between $300,000–500,000 per day, and that over 70 per cent of the sales were contributed by cannabis, ecstasy and cocaine products. It was also possible to identify both highly specialised sellers and sellers offering a large number of different products. Only a few members achieved very high earnings (> $10,000), while the vast majority earned less than $10,000 during the two years the study ran. It was further noted that anonymous online markets are fairly resistant to attacks (cf. Soska/Christin 2015: 34). This study is characterised by a detailed critical description of the methodology used in collecting and analysing the data. Based on that description, the estimates for the earnings tended towards the conservative, i.e., only amounts meeting certain criteria were included (cf. Soska/Christin 2015: 38). Furthermore, taking one category as a measurement or validation parameter — in this case, for example, the feedback from a customer being taken as definite proof that a sale had been completed — may be interpreted differently in other studies.

Kruithof et al. (2016) conducted a large empirical study of the magnitude and extent of the drug trade conducted over the Internet (cf. Kruithof et al. 2016: xxiii f.). To collect their data, they used the “DATACRYPTO” software developed by Decary-Hetu and Aldridge in 2013, which systematically archives websites and extracts relevant information such as product title and description, price, etc. (cf. Kruithof et al. 2016: 11). The collected data was then fed into a database, and this allowed cross-market searches for specified sellers, buyers and products to be carried out. From the eight markets
analysed in the study, over 105,000 listings were saved, and about 5,000 sellers identified (cf. 
Kruithof et al. 2016: 11 f.). At the beginning of the evaluation, the authors made several assumptions: 
for example, instances of customer feedback were taken as indications of completed sales 
transactions, and they were also used to calculate a seller’s monthly earnings (cf. Kruithof et al. 2016: 
16). The country from where a member dispatched his products was considered to be his “operational region” (cf. Kruithof et al. 2016: 17). The authors used the key for the encryption 
software "Pretty Good Privacy" to identify users who were active on several online platforms (cf. 
Kruithof et al. 2016: 19). A total of around 50 cryptomarkets and individual seller shops were counted 
in the darknet (cf. Kruithof et al. 2016: 102). About 57 per cent of the products of offer were 
narcotics (cf. Kruithof et al. 2016: 100). Only two per cent of the transactions analysed involved sums 
of more than $1,000 and were thus considered "wholesale" (so-called sale for resale). Even though 
these wholesale transactions made up only a small proportion of the total number of transactions, 
they accounted for about a quarter of total earnings from narcotics (cf. Kruithof et al. 2016: 101). The 
authors took the view that particular caution must be applied in a quantitative analysis of "big data" 
regarding the size and extent of online markets, which is why a manual review and adjustment was 
made necessary (cf. Kruithof et al. 2016: 13). An added factor was that the assumptions made prior 
to the analysis could be subject to criticism. One example of this is that it is not possible to determine 
for sure whether a user was active on several platforms based on the pgp-key alone, as profiles could 
be on-sold, or several protagonists could share a single key.

For their international study, the authors of the Cyber-OC report evaluated over 40 completed 
investigations from Germany, the Netherlands and Sweden and conducted interviews with experts 
and workshops. The data collected allowed the phenomenon Cyber-OC to be analysed in detail (cf. 
Bulanova-Hristova et al. 2016: 3). The study confirmed that, among other things, that illegal online 
platforms were used by cybercriminal groups for the trade in illegal goods and services or to identify 
ew group members or short-term supporters (cf. Bulanova-Hristova et al. 2016: 91 f.). The authors 
stressed the qualitative and exploratory nature of their study and listed potential sources of errors in 
their data collection and evaluation which could arise, for example, from the fact that they only 
analysed investigations that were able to be identified with the assistance of different security 
agencies. In addition, many investigation records lacked sufficient information about the individual 
suspects or about the entire group, but in many cases the information could be supplemented 
through interviews with the lead investigators.

5. The online black market – an overview

The Internet offers an ideal platform for all kinds of trade. In addition to the trading opportunities on 
legal Internet forums and marketplaces, there are illegal online platforms hosting a trade in large 
numbers of criminal goods, stolen data and criminal services. The criminal goods may be offline 
products such as narcotics or weapons on the one hand, or digital products required to commit 
cybercrime in the narrow sense on the other (cf. Hutchings/Holt 2014: 1).

The authors of the RAND report of 2016 identified a total of around 50 cryptomarkets in the darknet 
(cf. Kruithof et al. 2016: XXV). However, this number must be seen as a rough indication only, since 
one of the special characteristics of illegal online platforms is their volatility (Europol 2016: 47). Since
the first online marketplace for the narcotics trade went online in the Tor network in 2009 (cf. Buxton/Bingham 2015: 6), dozens of other online platforms have appeared, most of which disappeared again in a matter of months following measures taken by law enforcement authorities or as a result of so-called exit scams on the part of the administrators (cf. Kruithof et al. 2016: XXV). Illegal online platforms also exist on the clearnet, however. For example, the European Monitoring Centre for Drugs and Drug Addiction (EMCDDA) identified about 650 web shops for narcotics in the freely accessible Internet in the year 2013 (cf. Kruithof et al. 2016: 1). The authors of the Trend Micro report on Germany’s cybercriminal black market reckon that there are at least ten major German Internet forums and at least two German marketplaces where not only tools for committing cybercrime in the narrow sense are sold, but also other illegal goods. The illegal Internet forums identified in that report included around 70,000 registered users (cf. Trend Micro 2015: 5).

Based on estimates by Kruithof et al. and by Soska/Christin, around 60 to 70 per cent of the product listings on illegal online platforms on the darknet concern narcotics (cf. Kruithof et al. 2016: XXV and Soska/Christin 2015: 34). This means that narcotics are the type of goods sold most frequently by far, but there is a steadily increasing range of other products on offer as well. While weapons only represent a small fraction of the goods purchased on online platforms, the trade in weapons is particularly dangerous. In addition, there is trade in (forged) identity documents, stolen credit card information and cybercrime tools (cf. NCA 2016: 41). While some illegal online platforms are limited to trading in one field of crime only, others cover goods and services in various fields of crime.

There are open and closed illegal online platforms which can be utilised with or without prior registration with a profile. A further distinguishing characteristic according to Hutchings/Holt is the language used on the platform, which leads to the emergence of regionally limited black markets offering region-specific criminal services and goods – for example, many marketplaces are specialising in the trade with credit card data from a specific country (cf. Hutchings/Holt 2014: 7). As well as the international English-language underground economy, the Brazilian, Chinese, Japanese, French, German and Russian online black markets are also of significance. Trend Micro was able to document close links between the German and the Russian black markets in particular which manifest in the similar design and structure of the individual online platforms among other things. The authors of the Trend Micro study assume that German cybercriminals regularly visit Russian black markets in order to gain new ideas and concepts. The authors also make reference to a direct criminal cooperation between German and Russian online platforms, and in 2015 they were able to identify around 300 protagonists who appeared in both underground markets (cf. Trend Micro 2015: 37 f.). Even though German illegal online platforms specialise in services and products for the German-speaking region, they are usually registered and hosted outside the EU so as to evade surveillance by the German security agencies (cf. Trend Micro 2015: 15). While exact replicas of many of the German illegal online platforms also exist in the Tor network, the Russian underground forums made very little use of the deep web; they were usually located in the clearnet (cf. Trend Micro 2015: 12).

The earnings achieved on online platforms are considerable. It is estimated that in the two-and-a-half years that Silk Road existed, earnings totalled around 214 million US dollars (cf. Soska/Christin 2015: 40). For eight more online platforms analysed in 2016, monthly earnings of around 10 million euros were calculated (cf. Kruithof et al. 2016: XXV). Buyers most commonly paid in crypto currencies, i.e., with digital means of payment that can be used anonymously and in a decentralised manner (cf.

A further characteristic of the online black market is its steady growth. The authors of the RAND study were able to record a doubling in earnings from the online drug trade and a tripling in the number of transactions between 2013 and 2016 (cf. Kruithof et al. 2016: XXVI). Ablon et al. assume that the number of users of illegal online platforms will continue to rise, due on the one hand to the rapid increase in the range of websites and chat channels available, and the fact that "digital natives" are less afraid of the technical challenges on the other. However, the number of highly qualified participants has also risen markedly in recent years, and along with it the quantity and quality of the services offered (cf. Ablon et al. 2014: 5 f.).

6. Illegal online platforms structuring criminal activities

Criminal structures on illegal online platforms may on one hand encompass the mechanisms, rules and social process on the platforms themselves (Chapter 6), and on the other the criminal cooperation between different protagonists within different forms of collaboration – e.g., collaborative networks, hierarchical groupings of perpetrators or even traditional OC groups (Chapters 7 and 8). While the former describes how these online platforms are structured and how they facilitate criminal cooperation as a result of that structure, the latter focuses on independent groups of perpetrators on these platforms. Some authors therefore regard the illegal online platforms themselves as a form of criminal network, while for others they represent a type of sphere of activity for criminal groups. However, as illegal online platforms differ in terms of their structure and the mechanisms and rules they have in place, the following comments do not apply to all platforms in equal measure (cf. Kruithof et al. 2016: 24 f.).

6.1. Protagonists and their tasks within the platform-internal hierarchy

Many authors agree that illegal online platforms have a complex organisational structure and a clear division of responsibilities (cf. Holt 2013: 156). Most of them have a strict hierarchical structure (cf. Lusthaus 2012: 80) that allows them to exert formal control over the members and enforce the rules (cf. Yip et al. 2013: 4 f.).

‘One of the most distinctive characteristics of forums is the inherent hierarchical management system.’ (Yip et al. 2013: 4)

Ablon et al. were also able to show that online platforms frequently have a hierarchical organisational structure. This hierarchical structure is reflected in, among other things, the manner in which criminal earnings are distributed, so that a protagonist positioned at a higher level within the hierarchy of an online platform (administrators, moderators and testers) will receive a greater share of the earnings obtained through registration fees and/or commissions on completed sales (cf. Lusthaus 2012: 90).
It has also been shown that the strictness in terms of rules of access and behaviour varies depending on the level within the hierarchy (cf. Ablon et al. 2014: 5). The authors of the Trend Micro study refer to this as tiered access to online platforms. Whereas users with special knowledge, skills or connections may be given access to closed sections following a review by an administrator or a moderator (cf. Lusthaus 2012: 80), other users only have access to the open parts of the forum. Accordingly, a number of online platforms merely require users to register, whereas for other platforms a targeted invitation is a prerequisite for joining (cf. Trend Micro 2015: 12). Decary-Hetu and Dupont noted that it can often be a lengthy and difficult process before a member can become part of, or interact with, the higher levels of a hierarchy. A prerequisite was long-term, intensive participation in the online platform as well as earning a reputation which in turn depends on a member’s reliability (cf. Decary-Hetu/Dupont 2013: 6 ff.).

In the specialist literature, hierarchically structured illegal platforms are perceived as pyramid-shaped, akin to OC groups. According to Yip et al., one or more administrators are situated at the top of the online platform (cf. Fig. 6). They are responsible for the management and have full access to the internal infrastructure. They set the ground rules for accessing and using the platform and make long-term strategic decisions regarding, among other things, adequate protection mechanisms against law enforcement authorities or other competing platforms (cf. Yip et al. 2013: 4). Their responsibilities also include the control and sanctioning of the members of the platform. Based on the information available to them, they are able to vet specific vendors regarding their trustworthiness and distinguish or reward them accordingly (cf. Holt 2013: 165 ff.). In addition, they safeguard standards in terms of truthful and orderly communication and they can remove inappropriate offers or postings (cf. Hutchings/Holt 2016: 2). The option to exclude users from a platform following proven incidents of fraud is one of the most effective functions of an administrator, because doing so can counteract any destabilisation of the entire forum (cf. Holt 2013: 165 ff.). In many instances they receive a commission from every sale conducted via their marketplace (cf. Kruithof et al. 2016: 75).

Within the group hierarchy, moderators are positioned directly below the administrators. They frequently act as experts and are responsible for management, compliance with rule and maintenance of sub-sections of the online platform (cf. Hutchings/Holt 2014: 15 f.), these sub-sections being allocated to them based on their technical or specialist skills or their geographical location (cf. Ablon et al. 2014: 5). They determine whether postings to threads or product offers are in accordance with the rules and can delete inappropriate offers or postings (cf. Yip et al. 2013: 4). In addition, they often handle customer relations. Their access to the platform-internal infrastructure is limited, however (cf. Kruithof et al. 2016: 75).

On many online platforms, certain members also act as reviewers, in addition to the administrators. As an independent third party, they review goods and services offered by new members who want to become active as sellers, and in some cases they also offer so-called escrow or fiduciary services. Accordingly they perform an important function in establishing trust on their platform. They are often protagonists that are seen as being especially trustworthy by other members, protagonists whose recommendation will generally be followed by the other users (cf. Yip et al. 2013: 4). Many authors refer to them as intermediaries who often have above-average IT skills (cf. Figure 6) (cf. Ablon et al. 2014: 5).
The developers, also positioned higher up in the hierarchy, are responsible for the programming of the technical infrastructure of the online platform. They have extensive IT skills (cf. Kruithof et al. 2016: 75). In contrast, the so-called teachers write crime-specific instructions for other platform users and provide advice in order to facilitate the commission of various crimes (cf. Hutchings/Holt 2014: 15 f.).

**Figure 5: Typical hierarchy of a carding forum**

![Typical hierarchy of a carding forum](image)

Source: Yip et al. 2013: 4

The vendors and buyers using the online platforms for the illegal trade make up most of the rest of the users, and they are positioned at the lowest level of the hierarchy (cf. Figure 6). The vendors each have their own vendor profile on the online platform through which they are offering their goods or services (cf. Kruithof et al. 2016: 75 f.). While the administrators set the general rules applying to the entire platform, vendors can set their own terms and conditions for their sales and for returns (cf. Hutchings/Holt 2016: 2). Vendors offer criminal services, goods or data for sale. Data on offer is often obtained via data leaks, malware, phishing or skimming (cf. Hutchings/Holt 2016: 2). As their reputation is related directly and exclusively to their nickname, vendors who enjoy a good reputation will only rarely relinquish their nickname (cf. Yip et al. 2013: 4). On some illegal online platforms, vendors must pay the administrators a fee for the infrastructure made available to them. Added to this in some cases is a commission that falls due on every successful sale (cf. Van Slobbe 2016: 79). Not only buyers but vendors can also frequently be active on several cryptomarkets. Depending on the platform, buyers can avail themselves of more or less sophisticated and extensive feedback mechanisms through which they are able to rate vendors regarding their trustworthiness, reliability and product quality (cf. Kruithof et al. 2016: 59).

Also at the lowest level of the hierarchy are the so-called supporters acting as financial or goods brokers (so-called parcel or money mules), for example. In the German black market environment, the services of parcel mules are becoming less important as "packstations" can be used for the delivery or receipt of goods (cf. Trend Micro 2015: 21 f.).
There are also instances, however, where a member may perform multiple roles within a platform (cf. Hutchings/Holt 2014: 15 f.) Other protagonists whose contribution in the establishment and functioning of online platforms is of great importance, but who may not always be aware of the fact that they are participating in criminal activities, include the Internet service providers on whose servers the online platform is located. The same applies to suppliers of legal goods, e.g., envelopes for mailing narcotics, postal services, bitcoin\(^{10}\) currency exchanges, web design and advertising companies offering professional marketing services, etc. (cf. Kruithof et al. 2016: 76 and van Slobbe 2016: 79).

**Figure 6: Levels within an underground marketplace**

![Figure 6: Levels within an underground marketplace](source: Ablon et al. 2014: 6)

The hierarchical structure of online platforms facilitates swift and effective sanctioning whenever rules are breached. The most severe and most effective punishment is exclusion from the online platform (cf. Lusthaus 2012: 89). In many cases "fraudsters" are struck off the vendor lists by the moderators as a first step and subsequently excluded from the platform (cf. Yip et al. 2013: 4 f.). Moreover, online platforms also have their own "network boundaries" which also reinforce formal control and coordination: in many of the forums investigated, the administrators had the option of restricting access to the forum, for example, by preventing individual new members from entering, or even going as far as not accepting new members at all for a period of time (cf. Yip et al. 2013: 5). The regulation of trade on the platforms can also apply to the products being offered and may take the form of prohibiting weapons, stolen credit card information or child pornography to be offered for sale (cf. Kruithof et al. 2016: 25).

Lusthaus likens online platforms to mafia groups and their functions on the black market in the offline world. Just like mafia groups, online platforms facilitate and guarantee illegal transactions between criminals by setting and enforcing rules. Lusthaus adds that the similarities were even more striking where the online platforms collected fees and commissions (cf. Lusthaus 2012: 90).

\(^{10}\) "This is a currency which has neither banknotes nor coins. It consists of calculated, encrypted data blocks" (BKA 2016c).
These forums fit, at least partially, within the framework of the theory of protection. What these mechanisms demonstrate is an attempt to provide protection for cybercriminal transactions. In policing conduct and enforcing rules, administrators and other site officials are inserting a degree of trust into a world where such trust is largely lacking. In cases where third parties are available to guarantee transactions and where dispute resolution mechanisms exist, the forums may actually be approximating some of the functions performed by mafias in illegal markets. When they receive a ‘cut’ from these transactions, the similarities are even more apparent.’ (Lusthaus 2012: 90)

6.2. Reputation systems

Due to the anonymity of the users of online platforms, their physical remoteness and the illegality of their actions, neither legal remedies nor physical violence represent a viable means of enforcing agreements. Various regulatory mechanisms (cf. Kruithof et al. 2016: 23) in relation to the quality of the products and services traded as well as in relation to the reliability and trustworthiness of the members (cf. Yip et al. 2013: 3) are therefore necessary prerequisites for making cybercriminal cooperation possible in the first place (cf. Motoyama et al. 2011: 1). The proper functioning of illegal online platforms therefore relies on there being a certain level of trust, rather than on the latent threat of the use of violence as in the analogue criminal sphere. Reputation systems and rating systems therefore take on fundamental importance (cf. Cox 2016: 49 f.). They form the basis for making decision about purchases by the customers as well as decisions about whether to impose sanctions (cf. Kruithof et al. 2016: 85).

Ratings may take different forms, such as feedback or reviews of offers and vendors. They usually remain closely linked to the relevant nicknames and can also extend beyond the actual platform, so that they can also be found in social networks or on other websites, for example (cf. Cox 2016: 49 f.). A rating usually takes the form of giving a grade between one and five, with five representing complete satisfaction. Buyers are frequently requested to provide written feedback in addition to the numerical rating, covering various aspects of the order such as the quality of the product, anonymity and security during dispatch, the time taken for shipping, etc. Reviews are more comprehensive evaluations of certain products that are then published directly on the relevant platform or on other websites or in social media.

Reputation systems also provide potential customers with a retrospective overview of previous transactions conducted by a vendor and of the quality of his products. These means serve to gauge a vendor's trustworthiness and reliability (cf. Cox 2016: 53). For the vendors themselves, reputation systems provide a suitable avenue for demonstrating their reliability and hence look after their own reputation (cf. Yip et al. 2013: 8 and cf. Holt 2013: 165). A survey of Silk Road users from the year 2015 confirmed the significance of reputation systems: About two-thirds of the subjects surveyed indicated that existing reputation ratings as well as the option to rate vendors themselves were decisive factors in their decision to use this platform (cf. Cox 2015: 52).

As a rule, feedback tends to have a direct impact on the vendors within a marketplace in that those vendors attracting more positive feedback are contacted more frequently by potential customers (cf.
Holt 2013: 156). Unreliable or fraudulent vendors or vendors offering products of poor quality in turn are usually avoided by other platform members because of feedback (cf. Kruithof et al. 2016: 85).

Vendors’ ratings are not only based on the sale price. Good customer service and outstanding quality of the product or service purchased are often additional decisive factors in generating positive feedback. Buyers without technical skills in particular value it greatly. In most instances vendors offered dissatisfied buyers the option to exchange data they had purchased (cf. Holt 2013: 162). Some vendors went as far as guaranteeing their potential customers support in making use of the data, for example, in the cashing out of bank accounts, which had been sold as a service (cf. Holt 2013: 163). In addition, many vendors offered customer support (sometimes even 24-hour support) after the purchase of products or services, something that is particularly important for technically demanding goods (cf. Holt 2012: 8).

The speed with which a vendor provides answers to questions from potential buyers is considered to be the most important indicator for good customer service (cf. Holt 2012: 7 f.). The taken for delivery and the satisfaction with the quality of product or service purchased also played an important role. For vendors of DDoS in particular, the quality of the product was the main focus of their customer strategy. They let potential buyers do a 10-minute test run in order to check the efficacy for a specific target object. For cases where the purchased DDoS did not achieve the hoped-for effect, some vendors even offered a money-back guarantee. In some instances vendors offered free gifts in order to attract new customers (cf. Holt 2012: 7 f.).

A positive outcome of a vendor review by the administrators of a platform had the same effect as a formal quality guarantee (cf. Lusthaus 2012: 89). Yip et al. found that vendors who had been reviewed were contacted by customers much more frequently than those who had not been reviewed (cf. Yip et al. 2013: 8 f.).

A further type of feedback is the option to report fraudulent activities by users. Pertinent warnings to members can be issued in areas specially set aside for this purpose. This type of direct “complaint” also led to the establishment of trust within the platform (cf. Lusthaus 2012: 89). Members identified as fraudsters can then be excluded from the platform by the administrators. While a member expelled from a platform is free to re-register and create a new profile, he or she will not be able to use the old nickname because its reputation has been destroyed (cf. Ablon et al. 2014: 15).

The ratings system described here is not without its faults, however. For example, (fictitious) customers can make fraudulent claims or invent complaints in an attempt to inflict damage to competitors. Moreover, it is impossible to prevent even vendors who have been reviewed from defrauding their customers (cf. Cox 2016: 49 f.). To compensate for these possibilities, many platforms require that proof be provided in relation to the complaints raised (cf. Holt 2013: 165 ff.).

In this context, Motoyama et al. showed that a member's level of activity on a platform had a bearing on the whether his accusations were believed or not – e.g., complaints from a member with few contacts and a low level of activity on the platform against another member with a high level of activity did not succeed (cf. Motoyama 2011: 6). Many online platform also have mechanisms for conflict resolution that members can make use of (cf. Lusthaus 2012: 90).
The reputation mechanisms contribute towards the development of a so-called in-group identity which is characterised by features that are only known to members of the platform. This refers to specific patterns of behaviour, the language used (down to the level of the choice of vocabulary), and especially the combination of language, topics, interests, attitudes, knowledge, skills, etc. (cf. Lusthaus 2012: 82). This allows individuals "not in the know" to be identified quickly (cf. Yip et al. 2013: 7).

Despite the important function that reputation mechanisms fulfil in generating trust on illegal online platforms, The Economist points out that in the course of their activities many buyers would more often trust a particular vendor rather than the online platform as a whole. Among other factors, this is a result of the frequent shutdowns of the platforms by law enforcement authorities or by the administrators themselves (so-called exit scam). Kruithof et al. also refer to the fact that vendors and buyers who are active on illegal online platforms often establish close relationships, which in many cases leads to trading being moved from the platforms to other types of infrastructure, such as encrypted email. One example of this is the development which occurred after Silk Road was shut down (cf. Kruithof et al. 2016: 86 f.). Hutchings and Holt were also able to demonstrate that the negotiations and completion of a sale – that is, the transmission of the stolen data – often take place via private channels, rather than via the public forums where the initial contact was made (cf. Hutchings/Holt 2016: 2 f.).

6.3. Fiduciary systems

The fiduciary or escrow services made available by many online platforms also contribute towards making the cooperation between cybercriminals more reliable (cf. Trend Micro 2015: 21). This system benefits the buyers on online platforms in particular, as it provides them with financial security when making a purchase. The buyer ordering a product sends the money (e.g., in bitcoins) not directly to the vendor, but to a third party – e.g., the administrators of the online platform or some other intermediaries. The vendor will only receive the payment when the buyer confirms receipt of the product he ordered (cf. Ablon et al. 2014: 5).

Many platforms already feature more sophisticated escrow systems, however; these are so-called "multi-signature transactions", where two of the three participating parties (vendor, buyer and platform) must confirm the transaction before the funds can be transferred. This is intended to prevent, inter alia, that the administrators of the platform can withhold monies held in escrow in the event of an exit scam (cf. Cox 2016: 42). The inclusion of a third party results in greater organisational complexity for the illegal trade (cf. Holt 2012: 8 ff.). Moreover, it can increase the costs of the transaction since the escrow service usually needs to be paid for (cf. Holt 2013: 164). The intermediaries often receive a commission for their services which can range between three and 15 per cent of the transferred amount (cf. Trend Micro 2015: 21).

6.4. Quality control

An additional step in the effort to optimise services is the quality control system offered by some of the platforms. Administrators or some other trustworthy members of the platform check the quality of the products offered by vendors. The results of these tests are then communicated accordingly
and help potential buyers when rating the vendors in terms of their credibility and reliability. On other platforms quality controls are carried out on request (cf. Holt 2012: 8 ff.). In these cases vendors provide the reviewers with demo versions of malware or samples of their products (cf. Ablon et al. 2014: 15 f.).

The online platform “CarderPlanet” serves as an example of this. Peachey describes it as a strictly organised online forum based on the concepts and structure of the Cosa Nostra. To help make sure that members did not cheat each other, the forum offered a quality control system (cf. 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)

There is also a type of quality control that is not performed by the platform administrators but by the members and then made public in the form of lengthy postings or discussions. These discussion threads are of great relevance in the narcotics trade especially since they provided buyers and consumers with information regarding the "purity" of the narcotics, among other things (cf. Buxton/Bingham 2015: 11).

‘These are an important guide to the quality of products, reducing the likelihood of contamination, mixing and dilution with other products, overdose, and morbidity. Chat rooms and discussion forums enable information and experience sharing on drug safety, optimal dosing and polydrug use that reduce the risk of serious harm or illness.’ (Buxton/Bingham 2015: 11)

A further example of the commitment shown by members who were not part of the management level of a platform was the group "LSD Avengers". They subjected narcotics they had purchased on Silk Road to chemical testing. In this way they measured the quality of the narcotics, and they then published the results (cf. Ormsby 2016: 51). Based on the quality of the products, they then rated the narcotics vendors (cf. Cox 2016: 50 f.).

6.5. Digital contracts

Further stabilising mechanisms are the so-called “digital contracts” regulating various aspects of a cooperation extending over a period of time. The contractual terms and conditions are signed by the platform administrator by means of a PGP key. In the event of non-compliance with the contractual terms and conditions, the administrator acts as the dispute settlement or arbitration body. The user who failed to meet the conditions receives a pertinent notice on his vendor's page. In the case of a major breach a user can also be excluded from the platform (cf. Cox 2016: 53).

A good illustration of the regulatory system of carding forums is provided by Yip et al. Even though their exposition is based on carding forums where the bulk of the trade was in credit card information, it is applicable to most other forms of illegal online platforms. Yip et al. described the regulatory system provided on carding forums (cf. Figure 7), which in the authors’ opinion facilitates
the illegal trade considerably and which is also the main reason why the forums continue to be used by cybercriminals in spite of their weaknesses, such as being frequently shut down by law enforcement authorities or by the administrators (cf. Yip et al. 2013: 9). The reputation and escrow systems as well as the mechanisms for social networking – e.g., discussions, tutorials – are controlled and compliance with rules is ensured through the internal hierarchy and the fixed boundaries of the online platform. This reduces any uncertainty regarding the quality of the goods and the trustworthiness of the other protagonists ("identity uncertainty") (cf. Yip et al. 2013: 3).

Figure 7: Illustration of the regulatory system of carding forums

7. Online groups on illegal online platforms

The relevance of illegal online platforms for the preparation, execution and completion of cybercriminal activities is high. They facilitate and promote a collaborative approach that allows sophisticated cybercrime offences to be executed in the first place (cf. Holt 2013: 156).

The structuring and the organisational functioning of the platforms represent a significant danger, since they facilitate and promote the exchange between technically inexperienced cybercrime beginners and cybercrime experts with highly developed technical skills, and in doing so they organise the criminal relationships. Even though the purchase or sale of stolen data via illegal online platforms in itself is conducted by private individuals, according to Holt the selling process via an online platform should be seen as a participative and social process (cf. Holt 2013: 167).

Social networking between cybercriminals allows them to acquire social capital in the form of criminal resources and opportunities (cf. Yip et al. 2013: 5). Holt also comes to the conclusion that online platforms facilitate the commission of cybercrime offences (incl. identity theft) considerably by enabling extensive collaboration and the exchange of specialised knowledge (cf. Holt 2013: 167).
UNODC goes as far as referring to illegal online platforms as social networks of criminals who jointly and collaboratively commit crimes. In this endeavour, a few individual perpetrators or small groups (e.g., malware programmers and botnet operators) hold key positions around which the other protagonists are arranged (UNODC 2013 47 f.). This specialisation and division of labour on online platforms and in the underground economy in general has led to impressive productivity gains (cf. Yip et al. 2013: 1).

Online platforms first of all provide criminals with the opportunity to establish contact and recruit new members. They also function as a stable and relatively anonymous channel for communications, and they ensure the development of trust and sanctioning through forum-internal mechanisms. They facilitate and structure collaboration between criminals in that they allow them to join forces in a "project-specific" manner and without great expense with the aid of the illegal online platforms. In addition, online forums make it possible to market, sell and buy crimeware. Also on offer are comprehensive instructions which allow budding cybercriminals to acquire the necessary technical skills (cf. Europol 2011: 6).

According to Europol, the profit-oriented exchange between cybercriminals with varying levels of IT skills, which in this magnitude has only become possible since the advent of online platforms, represents a particular threat to governments, businesses and ordinary citizens. As can be seen in Figure 8, many cybercriminal activities require a complex form of collaboration, with each member of a group being assigned a specific role (cf. Europol 2015: 50). A similar distribution of roles within an illegal online market was also identified by UNDOC:

‘A cybercrime ‘black market’ has been characterized in which groups and individuals with different roles and sometimes acting in multiple roles (including ‘programmers’, ‘distributers’, ‘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 f.)

Figure 8: Groups of perpetrators formed on online platforms

Source: Yip et al. 2013: 1
Maximising profit is the top priority here. The members of a platform act in accordance with the rules of the market economy – the best offers succeed, and the system is continually optimised in order to increase profits further still. The highest earnings are said to be generated in the trade with, and the illegal use of, credit and debit cards (cf. Yip et al. 2013: 1).

The division of labour can consist of the participation of a continually changing set of fellow perpetrators who only participate in specific projects and for a limited period of time. However, this may also give rise to the development of groups that continue to operate over extended periods of time with the same set of perpetrators and the same allocation of roles. This latter situation mostly occurs where mutual trust among members and shared positive experiences foster a desire to develop a long-term collaboration. The authors of the Cyber-OC study refer to such groups as cyberborn. They may be groups whose members first met in an online environment such as a chat room, a social network or a forum and who later joined forces in order to commit cybercrime. The authors of the report note that such groups only rarely adopted a rigid hierarchical structure but were more likely to be organised in the form of networks operating in concert, where the division of labour was guided by the individual members' expertise, experience and access to technical and logistical means for committing a crime. This expedient flexibility did not get in the way of a structured approach; instead it enabled the groups to respond to internal and external influences in such a way that the commission of the criminal offences could be pursued in a more or less "person-independent" manner (cf. Bulanova-Hristova et al. 2016: 203).

8. Offline groups on illegal online platforms

Online platforms are used not only by individual perpetrators or so-called cyberborn groups, but also by previously existing, traditional OC groups. In the course of compiling this report, hardly any studies could be found that focused on the question as to how traditional OC is making use of illegal online platforms in the clearnet and the darknet for their criminal activities.

Due to the scarcity of reliable empirical studies, most of which are fairly recent, many authors came to the conclusion that the entry of "traditional" OC groups into cybercrime appeared uncertain and doubtful (cf. McCusker 2011: 116). Other authors are calling for theoretical considerations and assumptions about traditional OC groups entering into cybercrime to be backed by empirical data (cf. Lusthaus 2013: 52; Lavorgna 2016: 212). In this context it should also be taken into consideration that the definition of OC on which a study is based also becomes significant when investigating groups of perpetrators in the area of cybercrime (cf. Leukfeldt et al. 2016: 11).

International organisations like Europol (cf. Europol 2011: 5, Europol 2014: 11), INTERPOL (2016) and the United Nations Office on Drugs and Crime Control (UNODC) (cf. UNODC 2013: 44 f.) have been pointing out for years that "traditional", offline OC groups have entered into cybercrime. According to INTERPOL, they use the Internet to facilitate their criminal activities and maximise their profit within the shortest possible time. In many cases these activities are traditional crimes such as theft, fraud, illegal trade, whose scope and the extent of damage caused have increased markedly as a result of the new ICT technologies (cf. INTERPOL 2016). UNODC refers to cybercrime as a
transnational form of criminality and holds the view that its complex nature is further strengthened through the increasing involvement by OC groups (cf. UNODC 2016).

It states that in the case cybercrimes offering a high financial return such as computer fraud and identity theft, it must be assumed that the participation rate of conventional OC groups is very high (cf. UNODC 2013: 44). The Council of Europe came to similar conclusions as far back as 2004: OC groups were using the Internet amongst other things for drug dealing, for money laundering and to sell stolen goods, pirated copies or child pornography. They were also involved on a grand scale in sophisticated computer fraud and credit card fraud (cf. Council of Europe 2004: 119 ff.). In the majority of these modi operandi, online platforms played a more or less significant role.

‘Organised crime groups are especially involved in acts of sophisticated computer fraud, credit card fraud, and telephone fraud.’ (Council of Europe 2004: 119)

Traditional OC groups therefore do not only use the Internet as a means of committing crimes, but also in the commission of technically complex cybercrime in the narrow sense. Online platforms frequently play an essential role when traditional OC groups commit cybercrime in the narrow sense since they lower the bar enormously by allowing expertise, products, services or supporters to be acquired easily (cf. Europol 2014: 5).

‘[…] 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)

It is not necessary for the group's own members to possess any technical expertise, as financial or other means of exerting influence are frequently sufficient for OC groups to obtain the support of third parties (cf. McCusker 2006: 273).

‘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)

However, not all OC groups rely on “external” supporters or on products and services purchased via platforms. In their international empirical study, Bulanova-Hristova et al. were able to show that even traditional OC groups were able to draw on their own members for technical expertise (cf. Bulanova-Hristova et al. 2016: 214). In addition, an OC group can also “reorient” itself by specialising on technical modi operandi (cf. Tropina 2010: 1).

‘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 authors of the Group IB report on the Russian online underground market also come to the conclusion that online platforms in the clearnet and the darknet are used by traditional OC groups, and that these groups are capable of carrying out all the steps in the commission of a cybercrime independently. They suggest that this was leading to a merging of the offline and online spheres, with the effect that these groups were investing less in their traditional fields of activity such as dealing in drugs and weapons and prostitution and more in cybercrime (in the narrow sense) (cf. Group IB 2011: 7 and Essers 2012).
8.1. Number of OC groups active on online platforms

To date there have merely been attempts to estimate the proportion of users of underground markets made up by OC groups. These estimates are rarely reliable or generalisable since they are limited to platforms for certain product types and often refer to “organised groups” without specifying whether these are traditional OC groups or newly formed criminal online groups.

The authors of the Rand study on black markets hosting the trade with cybercrime tools and stolen data refer to an estimate according to which around one-fifth of the users on these markets belong to a criminal organisation (cf. Ablon et al. 2014: 4), but without specifying what kind of groups they were. The authors further assume that these market-internal groups will continue to grow as an ever-increasing number of platform members would join them (cf. Ablon et al. 2014: 4 f.). They add that these highly organised groups often also maintained links to traditional groups of perpetrators like drug syndicates, mafias and terrorist cells, and even governments (cf. Ablon et al. 2014: 39). However, the authors do not explain how they arrived at this estimate, or what these links look like in detail.

In its analysis of the darknet market archives, "The Economist" drew the conclusion that a group rather than an individual person was behind about 60 per cent of the vendor profiles in the darknet, as these vendor profiles used the words "we" and "us" (cf. The Economist 2016). However, the authors do not provide any information in relation to the number of group members or the type of group. It is therefore not clear whether they are offline groups or cyberborn groups. The authors do make the assumption, however, that the large drug syndicates, which to date have been dominating the narcotics trade, have not yet discovered the darknet for themselves. On the one hand they could continue to rely on their proven supply chains, and on the other, offline capabilities like violence, intimidation and smuggling were of no particular use in cyberspace. They specialise in dealing with narcotics in tonnes rather than in kilograms (cf. The Economist 2016).

8.2. Effects of OC involvement in illegal online platforms

In the literature the use of online platforms by traditional OC groups is usually only dealt with in connection with the illegal narcotics trade or cybercrime in the narrow sense. What is investigated frequently are the effects of the online trade with narcotics on the global and regional drug trade which is controlled by offline OC groups. This also raises the following questions: Does it exert pressure on the offline trade? Are traditional OC groups following suit and establish a second foothold on the Internet? Does the online trade even have an effect on the internal structure of traditional OC groups?

There is a consensus in the literature that the online trade for narcotics makes up only a small proportion of the global drug trade. Martin assumes that this proportion will continue to increase, however, and that this will force the various offline drug markets to adapt to this new development (cf. Martin 2014: 364). Online platforms are seen as having the potential to reduce the size and complexity of distribution networks, as technological progress allows for more direct connections between producers and end consumers (cf. Martin 2014: 364 f.). He suggests that the growth in the online trade with narcotics is turning the intermediaries and street dealers into the losers in this
development, because they become redundant in this leaner, more efficient supply chain (cf. Martin 2014: 365).

Based on their empirical study, Soska and Christin (2015) also make the assumption that cryptomarkets are competing mainly with street dealers, rather than with established offline OC groups specialising in the sale of large quantities of narcotics. They draw this conclusion based on the finding that the majority of online vendors earned less than $10,000 during the entire period they were monitored (2013-2015, 16 marketplaces) (cf. Soska/Christin 2015: 34).

Aldridge and Decary-Hetu (2014) arrive at a different assessment in their study of the Silk Road platform. Their assumption is that the narcotics trade on Silk Road was not exclusively a direct trade between producers and end consumers, but that they were often so-called business-to-business transactions. They say that many transactions would therefore take place between producers and intermediaries, which would mean that the online trade could easily involve groups from traditional offline Organised Crime. The authors came to the conclusion that between 31 and 45 per cent of the amounts of money turned over on Silk Road came from listings aimed at intermediaries rather than at end users (cf. Aldridge/Decary-Hetu 2014: 12). Indications that this may be the case can be seen in the language used on vendor pages ("dealer prices, "perfectly suited for resale"); the prices applicable to sales of large quantities, which were similar to street prices; discounts for large purchases; the sale of substances for further processing, etc. (cf. Aldridge/Decary-Hetu 2014: 10 ff.).

This would mean that the structure of traditional OC groups active in the drug trade could be altered in the long term as a result of the use of online platforms (cf. Aldridge/Decary-Hetu 2014: 6). They suggest that a new type of drug dealer was emerging, operating in a relatively violence-free market. The anonymity of online platforms was reducing the likelihood of physical violence, and that this also had an effect on the profile that a drug dealer needs to have. In this new era of the digital drug trade, new capabilities are required, such as good customer service and good writing skills, a good reputation as a vendor or a buyer (cf. Aldridge/Decary-Hetu 2014: 16).

As early as the year 2004 the Council of Europe pointed out that the commission of cybercrime could lead to changes in the structure of OC groups, as the hierarchical structure of certain OC groups could in fact be a hindrance with many of the modi operandi used over the Internet.

‘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)

"The Economist" also comes to the conclusion that the establishment and growth of the online trade with narcotics could have an impact on traditional OC groups, be it in terms of their internal structure or the perpetrator profiles they require. The authors also see a danger in that offline groups specialising in narcotics may make increased use of the darknet and relocate part of their trade there (cf. The Economist 2016).

Lewman assumes that such offline OC groups, which are already active in the illegal trade with goods, have already managed to expand their activities onto the Internet and on cryptomarkets with relative ease. As the main reasons for this, the author cites, among other things, the enormous profit potential and the reduced risk of being exposed to physical violence. Ross Ulbricht, the founder and
operator of the online black market Silk Road, is alleged to have had dealings with the Hells Angels organisation during his time as operator of the black market. During his trial it emerged that a Canadian chapter of the Hells Angels had supplied a Silk Road vendor with drugs; this can be seen as an example of how Organised Crime can step into cryptomarkets. According to this example, transnational OC groups mainly use cryptomarkets for the sale of various goods (often these are narcotics). Lewman writes that it was usually those members of an OC group who already operated successfully in "sales" in offline activities and who also had relatively good IT skills, which was a requirement due to the technical and organisational complexity of cryptomarkets (cf. Lewman 2016: 36 f.).

Kruithof et al. (2016) showed that large sales for amounts of more than $1,000, while relatively rare (two per cent of all transactions), generated about one-quarter of the total earnings on the online platforms that were analysed during the investigation period. Like Aldridge and Decary-Hetu, they draw the conclusion that is it likely that many customers on cryptomarkets are in fact drug dealers topping up their inventories for their offline sales (cf. Kruithof et al. 2016: xxvi). Moreover, they suggest that a proportion of the vendors are professional offline drug dealers who maintain close relationships with the producers and who operate in the online drug trade as an additional source of income (cf. Kruithof et al. 2016: xxix). One indication that this may be the case is the number of products offered. For example, the authors identified individual vendors who were offering several thousand listings (cf. Kruithof et al. 2016: 53). In addition, the earnings of the vendors can also be used as an indication of professional drug dealing. Of 2744 vendors investigated, about half earned less than $1,000 per month, whereas 51 vendors (around two per cent) earned over $100,000 per month (cf. Kruithof et al. 2016: 59). The authors then developed "markers/indices" that could indicate OC groups or professional brokers/intermediaries. The authors did not subsequently carry out a qualitative review, however.

Van Slobbe (2016) is somewhat more differentiating in his analysis. His assumption is that the online drug trade as a proportion of the overall drug trade is still too small (online drug dealers in the Netherlands achieved yearly earnings of around 30 million euros (cf. van Slobbe 2016: 77)) to have a severe impact on the profits made by the large offline OC groups (cf. van Slobbe 2016: 83). In the present situation, if a European OC group wants to import large quantities of narcotics from another country, a meeting is held between representatives of both parties in the lead-up. The basis for this exchange is trust, creditworthiness and strict sanctions in the event of rules being breached (cf. van Slobbe 2016: 128). This preparatory phase cannot easily be moved into cyberspace – the financial interests and risks involved would be much too high (cf. van Slobbe 2016: 78). Little has changed also in terms of the transportation of large orders, with shipping containers, airfreight or couriers still being relied on (cf. van Slobbe 2016: 78).

Only in the areas of mediation, initiation of business transactions and establishing contact were there indications that traditional offline OC groups made use of the opportunities offered by online platforms, in that it was possible to observe many online vendors offering sales of particularly large quantities (cf. van Slobbe 2016: 78). Criminal offline groups whose earnings are generated from the drug trade and who customarily defend their business model even using physical violence would not allow the online trade to restrict them in the longer term if their losses were to become too big (cf. van Slobbe 2016: 81).
Van Slobbe therefore also assumes that narcotics offered on online marketplaces even now are not limited to customer’s private consumption: for example, special offers apply for large orders (e.g., more than 5,000 ecstasy pills; over 500 grams of cannabis, etc.) (cf. van Slobbe 2016: 82). If the online trade were to continue to grow rapidly in the coming years, it had to be assumed that OC groups would also become increasingly active online and take over online platforms. Due to their central role and their comparative advantages in the import of drugs, they would succeed in forcing other online vendors out of the market. The belief that IT security measures would be able to prevent this from occurring was naive, since traditional OC groups were already using private servers and protected networks for communications within the group. Given this background, it was also conceivable that traditional OC groups would establish and operate their own cryptomarkets. If the online drug trade continues at the same level, then the probability that traditional offline OC groups would see their participation in the online business as profitable is quite low. This is also the reason why the author assigns a high priority to combating the current crop of cryptomarkets for the drug trade, as a way to stop traditional OC groups from getting more involved in the online trade (cf. van Slobbe 2016: 83).

Moreover, there is some empirical evidence which shows that OC groups have expanded their drug trading activities to include the online trade: Horne et al. investigated the efficacy of forensic information (geographical data, physical similarity of the packages, fingerprint traces, etc.) in the fight against the organised narcotics trade in Australia. They placed a particular focus on dispatch by mail as this was the most visible leg in the supply chain and because the inspection of intercepted packages and envelopes was one of the most effective measures for identifying the dealers (cf. Horne et al. 2015: 79). For up to three-quarters of the intercepted packages and envelopes containing narcotics the products had been purchased online (cf. Horne et al. 2015: 79). Following a close inspection of the intercepted packages – different fingerprints were found – it was possible to identify an Organised Crime group which had sent a large number of packages from Canada, among other countries, to different addresses in Australia. In addition to the fingerprints, it was also possible to collect nicknames which could subsequently be matched with profiles on Silk Road and Black Market Reloaded (cf. Horne et al. 2015: 79 f.). The authors described the group as a productive syndicate which, thanks to adapted forensic methods, was successfully located and eliminated (cf. Horne et al. 2015: 80).

In addition to the sale and purchase of various goods or data, such as weapons, narcotics or stolen credit card data (cf. Bulanova-Hristova 2016: 37 and 181) and criminal services, other reasons for using online platforms were identified on the basis of empirical analyses: OC groups use online platforms to, among other things, prepare cybercrime offences in the narrow sense (cf. Leukfeldt 2016: 38 and 93); recruit supporters such as money mules; acquire experts on a project-related basis, or identify new group members located in other countries or possessing specific skills sets (cf. Bulanova-Hristova et al. 2016: 94 and 120; cf. Leukfeldt 2016: 49 f. and 74 f.). In these circumstances, online platforms function as “universities for (cyber)criminals” – just like prisons do in many criminal subcultures – (cf. Leukfeldt 2016: 75), where members of OC groups were able to increase their skills and knowledge (cf. Bulanova-Hristova et al. 2016: 278).
9. Challenges and recommendations for action

In about half of the sources evaluated, recommendations for action were derived from reflecting on the challenges faced by the law enforcement authorities in cybercrime investigations in the field of illegal online platforms. These statements relate to measures relating to investigative measures, the positioning of the law enforcement authorities in terms of organisation and content, their cooperation with different protagonists, and future developments. The following section summarises the statements dealing with illegal online platforms in the clearnet and the darknet.

9.1. Potential courses of action for law enforcement authorities

Most darknet investigations conducted by European law enforcement authorities are directed against vendors and buyers on marketplaces for illegal narcotics. However, the illegal trade with weapons, unlawfully acquired data or other illegal products is also often at the centre of attention of the law enforcement authorities (cf. Europol 2016: 47).

The actions of the law enforcement authorities can be assessed against the background of situational crime prevention. Being part of secondary prevention, situational crime prevention is mainly aimed at reducing opportunities to commit crimes. This would lead to a situation where committing a crime was no longer a worthwhile endeavour for potential criminals due to the increased risk or due to a reduction in potential profits (cf. here and in the following: Kohl 2012).

9.1.1. Increasing the effort to commit the crime

Criminal networks specialising in the commission of technically sophisticated attacks – e.g., on bank customers – depend on having members who are able to use a multitude of different cybertools. The groups of perpetrators can usually purchase the required malware without great effort and expense via illegal online platforms. One way to increase the effort and expense involved in committing a crime by individual or groups of perpetrators is therefore the permanent disruption of the kind of criminal infrastructure where the necessary cybercrime tools are offered for sale. Leukfeldt assumes that malware designed to attack the online banking activities of Internet users would be distributed less rapidly and be deployed less frequently if the relevant online platforms hosting the trade in such malware were shut down by law enforcement authorities (cf. Leukfeldt 2016: 180).

The permanent closing down of online platforms is also portrayed as an important measure aimed at reducing the income of groups of cybercrime perpetrators. The objective is to prevent stolen credit card data, personal data, malware, botnets and other illegally acquired products from being sold easily and profitably. Doing so would eliminate the key incentive – financial gain – for the criminal groups. This could be achieved through the permanent shut down of a platform, by sabotaging the internal system designed to generate trust (by spreading false information) or by arresting key protagonists of the platforms, such as the administrators or top sellers (cf. Leukfeldt 2016: 181). Europol notes that shutting down or smashing illegal online platforms were among the core tactics employed by law enforcement authorities in the fight against illegal structures in the darknet. The inherent volatility of the online black market, which is reflected in the short-lived nature of many online platforms, among other factors, thus also works in favour of the authorities. Europol points
out that in the year 2015 several illegal marketplaces closed down either as a result of exit fraud – so-called “exit scams”11 – or in order to fix alleged “security vulnerabilities”, and did so in the absence of any apparent action by law enforcement authorities. However, **internationally coordinated activities carried out by law enforcement authorities** also had destabilising effect. While the illegal online platforms still in place following Operation Onymous12 in the year 2014 were quickly able to recover and were joined by new platforms, according to Europol even today panic still spreads quickly among their members whenever a platform cannot be reached temporarily, as they are afraid that the platform has been shut down, or that there has been an exit scam (cf. Europol 2016: 47). A further negative consequence for the members that is associated with the shutting down of an illegal online marketplace was the potential **loss of bitcoins temporarily held in an escrow service** (cf. Ormsby 2016: 67).

However, in the specialist literature the closing down of online platforms is largely portrayed as futile, and sometimes even **counter-productive**. Several authors note that the online black market is fairly resilient and that it therefore will continue to exist despite raids and other measures taken by law enforcement authorities (cf. Aldridge/Decary-Hetu 2014: 18). On the contrary, shutting down a platform would only lead to the establishment of new and more professionally designed platforms (cf. Ablon et al. 2014: X). The shutting down of Silk Road resulted in, for example, the emergence of a virtually identical cryptomarket as well as several new, technically more robust competing marketplaces within a matter of just a few weeks (cf. Buxton/Bingham 2015: 14). This meant that the measures taken by the law enforcement authorities ultimately led to a fragmentation and diversification of the drug markets (cf. Buxton/Bingham 2015: 12).

> ‘Just as the interdiction and break-up of Colombia’s Medellin ‘cartel’ and assassination of its leader Pablo Escobar had no impact on levels of cocaine supplied from Colombia, so closing Silk Road and arresting Dread Pirate Roberts had no long term or catastrophic impact on the Silk Road project or hidden markets more broadly; quite the reverse. It stimulated new competition, innovation in business models and the launch of Silk Road 2.0.’ (Buxton/Bingham 2015: 14)

The closing down of Silk Road in 2013 thus did not have the intended effect, as illegal narcotics (and other goods) were still able to be traded online on one of the 20 newly established markets (cf. Ormsby 2016: 66). **To produce a more accurate estimate of the potential impact of specific countermeasures, a comparison of multiple scenarios would appear useful.** Closing down an illegal online platform can in theory result in the following outcomes: vendors and buyers can move to another existing web page, or they can develop a new cryptomarket where the same community can become active again, or they can cease their online trading. Given the mutual dependencies between vendors and buyers, the risks associated with moving to an unfamiliar marketplace, and the compulsion to consume drugs, the second option appears to be the most likely (Van Slobbe 2016: 81).

Interviews conducted with Silk Road users shortly after the platform was shut down showed that some members experienced the effects as negative, and they returned to buying and selling offline. For many others, however, it was merely seen as a temporary inconvenience, as they were quickly

---

11 A type of fraud where a vendor or an online platform ceases operation without prior notice, having financially enriched themselves by exploiting the trust of customers, e.g., through the provision of an escrow service (cf. Kruithof et al. 2016: xxxiv).

12 Shutting down of 27 webshops in the Tor network and arrest of 17 suspects in various countries (cf. Beuth 2014).
able to move the trade elsewhere and continue their trading operations. This was partly due to the fact that some members had already been active in several cryptomarkets, and by checking the encrypted signatures of other Internet users they were able to ascertain that these were the same users even on the new online platforms. There were also instances where users no longer relied on illegal online platforms. Former Silk Road vendors built their own websites independently of established online markets and encouraged their former buyers to contact them in future using encrypted email. In doing so, they moved their communications even further "underground" (cf. Kruithof et al. 2016: 103). This was successful especially if there were pre-existing relationships based on trust between vendors and buyers (cf. Ormsby 2016: 66). Moreover, the actions taken by the law enforcement authorities led to users making even greater efforts to ensure their own security (cf. Buxton/Bingham 2015: 13).

Instead of the complete shutdown of a large number of online platforms, as happened during Operation Onymous and which was both time and resource-intensive, many authors take the view that new kinds of countermeasures ought to be considered (cf. Soska/Christin 2015: 46). Soska and Christin see greater promise in a reduction in the demand for illegal narcotics as a result of effective preventive measures. They also suggest that more targeted and more precise investigative measures in traditional police work, such as the interception of particularly hazardous products in the mail, could achieve more than a complete shutting down of these platforms (cf. Soska/Christin 2015: 46).

Many authors recommend disrupting the reputation systems on illegal online platforms. One promising approach they suggest is the undermining of trust between members, since trust is essential if transactions are to be successful. This method would have a negative impact on the efficacy of the entire platform in the long term (Holt 2012: 11). Van Slobben takes the view that it would therefore be worthwhile to develop strategies capable of severely undermining the trust in the illegal online platforms on the part of vendors and sellers in general, leading to a decline in their use (cf. Van Slobben 2016: 82).

Other authors are of the opinion that the evaluation and analysis of operational platforms was more effective in the long term than the shutting down of a few important online platforms. Cataloguing or building an inventory of criminal structures within the platform and of the conduct and collaboration of the members could, for example, be used to successfully develop covert identities for the law enforcement authorities. Such comprehensive information could only be obtained by constantly monitoring several online platforms as well as the conduct of their members. This would also make it possible to discern differences between the various subcultures and market forces. Moreover, with the help of specially trained covert investigators it would be possible to collect valuable information pertinent to the identification of platform members and to detect new developments at an early stage (cf. Holt 2013: 169). Obtaining information via online platforms is of great importance since, in contrast to other channels of communication such as Internet Relay Chat, they are easier to monitor and analyse. This was significant especially in cases where Internet users were operating on both channels (cf. Yip et al. 2012: 65).

The specialist literature also made reference to the need for proper prioritisation. It was important that law enforcement authorities continue and step up investigations into the providers of important criminal cyber tools and services, such as developers, vendors and buyers of malware and vendors of DDoS services. The elimination of these highly specialised protagonists and services would
have a significant impact on the cybercrime community and prevent millions of cyber attacks (cf. Europol 2016: 12, 15, 23). It was also suggested that **not only should users of malware be punished, but programmers as well**. This approach was thought to be particularly promising as the number of highly qualified cybercriminals overall is quite limited and their skills are difficult to replace. According to Europol, many of the particularly dangerous malware variants are controlled by closed criminal groups, and their elimination could seriously damage the online black market (cf. Europol 2014: 14).

### 9.1.2. Increasing the risks of committing the crime

Because they act as both marketplaces and digital meeting places or forums, illegal online platforms play a key role in the formation of cybercriminal networks. Leukfeldt therefore takes the view that a **formal surveillance of these places could prevent, among other things, the creation and continued development of cybercriminal networks** (cf. Leukfeldt 2016: 181). Successful surveillance requires close cooperation, coordination and a lively exchange between law enforcement authorities in a national and international context. In doing so, the focus should be on **administrators, moderators, the main vendors** (cf. Van Slobbe 2016: 82) and on **particularly respected and trustworthy members** (cf. Holt 2012: 11).

Many online platforms have a large number of international members, and participating groups of perpetrators are also frequently spread across several countries. The international scope of cybercrime in terms of the suspects, the crimes and the victims meant that it could only be countered effectively through international cooperation. Investigations of cybercrime should not end at national borders but should involve all the countries in which the perpetrators operate (cf. Bulanova-Hristova et al. 2016: 87). Furthermore, it was important that the **law enforcement authorities continue to invest in research and development in big data** so as to ensure that effective techniques for mapping nicknames and criminal activities to IP addresses can be developed (cf. Van Slobben 2016: 82). In addition, future research should be conducted with the aim of developing the ability to trace malware used in cyber attacks on business or private Internet users back to the sales platform and to its developers and vendors. The same applied to other illegal goods such as weapons, raw materials for drug manufacture, etc. Holt writes that it is important to **establish connections between criminal offences committed online and offline** (cf. Holt 2012: 11).

Furthermore, indications pointing to cybercrime should be noted even in investigations dealing with traditional groups of perpetrators (cf. Bulanova-Hristova et al. 2016: 212 f.). Having investigative measures referring both to offline and online environments of criminal groups would increase the level of risk to which the perpetrators are exposed considerably (cf. Leukfeldt 2016: 181).

### 9.1.3. Reducing the rewards of committing the crime

It is **at the transition point from the online to the offline sphere** in particular that law enforcement authorities are able to **intervene effectively in the criminal activities of platform users especially**. It is here that opportunities exist to identify perpetrators (increasing the level of risk) and reduce earnings (of a financial or material kind) (cf. Martin 2014: 358).
Several authors note that the moment where illegal goods enter the legal postal system is particularly well suited for the investigations by the law enforcement authorities. Conventional investigative measures are therefore of great importance in the detection of cybercrime (cf. Martin 2014: 354). Inspection of packages and envelopes should be professionalised and carried out on a regular basis (cf. Van Slobben 2016: 82). In this context Europol recommends that the law enforcement authorities gain an overview of all the "packstations" within their jurisdiction and work closely with the relevant service providers (cf. Europol 2016: 14). In addition, goods paid for with incriminated funds should always be seized (cf. Van Slobben 2016: 82).

Even though these measures are often among the most effective for identifying platform members, a number of authors note that they are associated with several problems. One of these problems is the enormous number of packages of this kind, and hence the danger that customs authorities could quickly become overwhelmed as a result (cf. Martin 2014: 354). And even if the police did manage to intercept a package containing illegal goods, in most cases the recipient's address would be false, making it difficult to identify the recipient. The effort and expenditure involved in conventional investigative measures employed to find the identity of the recipient, such as surveillance measures, observation, etc., would however only rarely be commensurate with the results obtained, since most consignments contain only small amounts of illegal drugs. Depending on the applicable legal provisions, those may be amounts destined for private consumption, in which case it is often decided not to prosecute (cf. Martin 2014: 360 f.). Moreover, in most cases vendor and buyer do not know each other personally, and for this reason they would not be able to provide any information about each other’s identity (cf. Martin 2014: 358).

An additional avenue for fighting cybercrime in the offline world is to prevent funds obtained through cybercrime activities to be withdrawn and passed on to the masterminds or backers. As an integral step of many cyber modi operandi, it represents a weak link in the criminal process. In addition to preventive measures warning citizens against acting as financial agents, this situation also offered the opportunity to cooperate closely with banks (cf. McCoy et al. 2012: 15). The specialist literature also recommends that amounts of cryptocurrencies that can be attributed to users of illegal online platforms should always be confiscated, and that service providers for cryptocurrencies supporting the illegal narcotics trade should be dismantled (cf. Van Slobben 2016: 82).

9.1.4. Reducing incentives and removing any excuses

Members of cybercriminal networks spend much time in chat rooms and on forums offering extensive instructions for cybercrime in the narrow sense, and which were therefore replacing prisons as "the universities for criminals" (cf. Beiersmann/Espiner 2011). The information conveyed includes details of vulnerabilities in current versions of software, or instructions for using different cybercrime tools, i.e., knowledge that is often of great importance for individuals and groups of cybercriminal perpetrators. However, Internet users who do not have a criminal background also move in this "cyber subculture" with its diverse range of discussion groups and forum contributions. The normality with which the exchange of information about criminal projects and activities proceeds thus leads to a shift in perception about what is legal or illegal. An added factor is that the victims (e.g., bank customers) become "dehumanised", as the discussions merely refer to amounts of money that need to be transferred. There is also easy access to a range of low-cost offers of illegal
goods and different support options for the commission of cybercrime in the narrow sense. In this context, several authors agree that these constellations would induce many Internet users without criminal intentions or background into committing cybercrime (cf. Leukfeldt 2016: 182 f.).

They therefore stress the special importance of reducing the incentives for using illegal online platforms and eliminating excuses for committing criminal activities. This can be achieved by means of comprehensive education campaigns targeting potential perpetrators and explaining to them that cybercrime involves actual criminal offences with real victims (cf. Leukfeldt 2016: 182 f.). Potential victims and/or potential supporters could be reached via preventive awareness campaigns like the "Don’t be a money mule!" campaign run by Europol, which highlights the dangers of acting as a financial agent (cf. Europol 2016: 12). Campaigns such as these must explain the consequences of cybercrime for the victims and the perpetrators in an easy to understand manner (cf. Europol 2016: 13) and draw attention to the fact that acting as a money or parcel mule is illegal and in most cases is supporting serious Organised Crime. Last but not least, the awareness campaign should deter Internet users from committing criminal offences and potentially joining a criminal cybercrime group (cf. Leukfeldt 2016: 182 f.).

9.2. Positioning of the law enforcement authorities

Most criminal activities on illegal online platforms are directly related to offline crime – for example, the online trade with narcotics, weapons, counterfeit money, and stolen data. According to Europol, this highlights the need for all sections of the law enforcement authorities to have the capability to conduct online investigations, as cybercrime also plays an increasingly important role in many "traditional" areas of offline crime – as for instance in human trafficking, narcotics, weapons, economic crime, terrorism (cf. Europol 2016: 48). This requires adjustments to training and appropriate further training measures (so-called "capacity building") through which the requisite knowledge and skills can be taught. It should be ensured that investigators working in various areas of crime possess basic knowledge of IT forensics, that is, in the collection of digital traces and the seizing of digital goods and currencies (cf. Europol 2016: 13). Europol holds the view that the law enforcement authorities must counter the rise in cybercrime in both the narrow and the broad sense with a commensurate increase in adequate resources and skills (cf. Europol 2014: 14). It is also pointed out that financial investigators need to receive additional training in the tracking, seizure and investigation of virtual currencies (cf. Europol 2016: 13), as the depiction of money flows represents an important measure in criminal court proceedings and one that ought to be used extensively by law enforcement authorities (cf. Meiklejohn et al. 2013: 2).

Buxton and Bingham raised the question as to whether the law enforcement authorities (in the United Kingdom) actually possessed the necessary resources to mount an effective surveillance of the cryptomarkets (cf. Buxton/Bingham 2015: 18). They take the view that what is needed is a prioritisation of the areas of crime. They recommend that the limited resources are focused on cybercrime that is dangerous, organised, or involves great financial losses – e.g., sexual exploitation of children and women, economic crime, the weapons trade, cross-border cyber attacks, cyber

---

terrorism. The decision about which investigative measures were to be taken had to be based on a tiered cyber risk assessment: for instance, in their view violence-free drug trading on self-regulating online platforms where no other types of goods are traded was of little relevance, compared to other types of crimes which generate higher illegal earnings and represent a greater potential threat to society (cf. Buxton/Bingham 2015: 20).

In addition to calling for comprehensive training to impart knowledge and skills in IT forensics and the prioritisation of areas of crime, the literature also frequently contains recommendations demanding additional skills and improved capacities for cyber investigations. Because even though online platforms create space for advertising and the establishment of collegial (criminal) relationships, the trading and the collaboration often take place outside the forums or marketplaces, involving just a few participants, e.g., via private messenger services. The latter are difficult or impossible to monitor for law enforcement authorities (cf. Holt 2013: 164). The encryption of many online platforms by Tor makes it difficult to identify vendors and buyers and to track their overall activities (cf. Martin 2014: 357). This makes apparent the necessity for law enforcement authorities to have up-to-date and adequate tools, techniques and expertise at their disposal, so as to be able to take action against the criminal use of encryption and anonymity (cf. Europol 2016: 12). This includes the development and deployment of IT forensics standards and procedure to facilitate cross-border investigations and the exchange of digital evidence and ability to rely on own staff with special skills and knowledge in rare languages and in the phraseology and jargon used in cyber subcultures (cf. Europol 2014: 14).

9.3. National and international cooperation

Given the transnational character of the illegal online platforms, most of the authors agree that national police strategies and investigations alone will not be enough to combat this type of crime effectively (cf. Buxton/Bingham 2015: 17 f.).

Buxton and Bingham note that in many cases the fight against the darknet is confined to a national context, without sufficient international coordination (cf. Buxton/Bingham 2015: 12). They state that cross-border cooperation frequently remained a big challenge, be in terms of the responsibility in international investigations or due to legal differences (cf. Buxton/Bingham 2015: 18). Effective international cooperation would continue to be hampered by differing national priorities and legal requirements. This observation can be illustrated using the example of the fight against the narcotics trade. While the EU countries agree that investigations should focus on producers, main distributors and intermediaries because of the very negative effects their activities have, when it came to dealing with end users, opinions and approaches differed, according to Van Slobbe, who notes that international discussion and coordination were virtually non-existent in this area (cf. Van Slobbe 2016: 77 and 81).

There is a consensus in the specialist literature that in the fight against illegal online platforms, an intensive international, or at least European, exchange between national law enforcement authorities is of particularly high relevance. Especially in international investigations there was a need for cooperation to proceed more swiftly and be less complicated. To this end, existing cooperation agreements should be reviewed in detail and adapted accordingly to allow individual
and groups of perpetrators on illegal online platforms to be effectively identified and convicted (cf. Holt 2013: 170).

Optimisation in this area would result in a number of improvements: for example, exchanges on a regular basis would lead to the elimination of duplication in investigative work and create synergies to be exploited (cf. Europol 2016: 48). Moreover, such measures would **significantly enhance trust between the national authorities, and this would lead to an actual transfer of know-how and investigative findings, and hence to a better understanding of the scale of the threat. Especially a standardised exchange regarding current developments or strategies can have a positive effect in this regard** (cf. Europol 2014: 14). However, international cooperation should be intensified not only between EU countries, but should be expanded to include countries from where cybercriminal perpetrators and groups are operating, e.g., where money is withdrawn or goods are received (cf. Europol 2016: 13). **Europol and INTERPOL provide their member states with several structures supporting a practical exchange of views and experiences, as well as with mechanisms for cooperation.** In addition, they pool relevant information – e.g., reports on newly emerging cybercrime developments and pattern of attack – and handle the coordination of joint actions conducted by national law enforcement authorities. The objective here is to make optimal use of limited resources (cf. Europol 2014: 14).

The specialist literature frequently refers to the necessity for **stronger cooperation between law enforcement authorities and other stakeholders in society in combating crime in relation to illegal online platforms.** For Europol the exchange of information and findings with scientists and researchers as well as with private security agents is important in terms of gaining an overview of current and relevant findings that is as comprehensive as possible (cf. Europol 2016: 13). Especially for crimes involving payment cards, close cooperation with private agents in relationships based on mutual trust were of great importance. Considered on its own, a case of credit card fraud tends to be assigned a relatively low priority. Due to the fragmented nature of this type of fraud (victims can be spread across the entire nation or throughout the whole of Europe), connections between individual cases may only be identified at a late stage. **A timely exchange with financial institutes can help identify groups of Organised Crime that are involved in payment card fraud** (cf. Europol 2016: 13).

The literature also suggests that law enforcement authorities should intensify cooperation with private agents who are responsible for managing and maintaining important parts of the Internet. This was necessary because digital evidence could often only be obtained via these agents. One way to achieve this would be for **law enforcement authorities to enter into a public-private partnership with Internet providers.** This would make it easier to persuade providers who are unwittingly hosting cryptomarkets to refrain from doing so (cf. Van Slobben 2016: 82). The same applies to the contact with parties providing virtual currency exchange services (cf. Europol 2016: 14). In addition, investigations should be launched into businesses that are quite deliberately hosting cryptomarkets (incl. so-called "bulletproof hosts"). Moreover, their activities could be restricted by making them subject to approval regulations (cf. Van Slobben 2016: 82).

Law enforcement authorities in Europe consider the limitations to darknet investigations resulting from national laws and regulations to be one of the greatest challenges (cf. Europol 2016: 47 f.). A quarter of survey participants even stated that they were **definitely hampered in their investigations by national laws and regulations** (cf. Europol 2016: 48).
‘The majority of law enforcement investigations on the Darknet focus on markets selling illicit drugs – or at least the vendors and buyers thereon. Those selling weapons, compromised data or other illicit products such as pharmaceuticals and chemicals are also key targets for law enforcement. One of the main challenges for law enforcement in this area – aside from the additional attribution issues – is the ability to operate lawfully in these environments, with one quarter of respondents clearly restricted by their national legislation.’ (Europol 2016: 47 f.)

Buxton and Bingham also refer to the fact that measures taken by law enforcement authorities against the darknet can often only operate within narrowly defined legal boundaries (cf. Buxton/Bingham 2015: 12). Among other things, Europol calls for legislators in the member states to provide their law enforcement authorities with effective legal instruments for investigating and eliminating cybercriminal activities efficiently (cf. Europol 2014: 14). Reference is made, for example, to the often inadequate laws governing data storage in the European countries, which is why a Europe-wide EU directive on data storage was a necessity (cf. Europol 2014: 70). Due to the international scope of many cybercrime offences, Europol calls for a uniform European legal framework which would result in a clear set of rules and avenues for investigation applicable to the whole of the EU. One step in this direction would be ratification of the Budapest Cybercrime Convention by all EU member states, for example (cf. Europol 2016: 48).

9.4. New developments

Operation Onymous demonstrated that illegal online platforms are not impenetrable. While care is taken that their physical location is and will remain unknown, they do require hosting on a server, and this provides the law enforcement authorities with an angle of attack. However, already a new type of illegal online platform – the so-called decentralised marketplace, e.g., OpenBazaar (cf. Muadh 2014) – has been developed that does not have this same vulnerability, since it operates on the basis of a peer-to-peer system. On the OpenBazaar platform, which can be accessed free of charge through a stand-alone computer software program, Internet users can search for products which they can then acquire directly from the vendors via multisignature transactions using bitcoins (cf. Europol 2016: 48, Van Slobbe 2016: 82 and Buxton/Bingham 2015: 15).

According to Europol there is as yet no certainty regarding means of investigation that can be successfully employed against decentralised illegal online platforms (cf. Europol 2016: 48.). However, Kruithof et al. assume that this new development has the potential to severely restrict the scope for action on the part of the law enforcement authorities in their investigations into, or the dismantling of, cryptomarkets (cf. Kruithof et al. 2016: 139).

In their article published in 2016, Soska et al. developed a theoretical concept for a decentralised anonymous marketplace offering better protection against attempts to manipulate members’ reputation compared to existing decentralised marketplaces, as well as offering greater anonymity. Participation in this platform, which the authors named "Beaver", was free of charge and did not require a third party to exercise control or establish trust. Here, too, vendors can gain trust by selling goods, yet, according to the authors, in Beaver’s case it was impossible to manipulate the reputation of a vendor by posting fictitious ratings. Compared with other decentralised platforms like

---

14 Systems or networks that do not rely on a central server but are distributed across several participants (cf. Kruithof et al. 2016: XXXV).
OpenBazaar, Beaver also allowed for significantly enhanced anonymisation, as nobody would know what goods were purchased by which customer, and nor can feedback be linked to specific transactions. The aggregate of the transactions (products offered for sale, payments, feedback) conducted via Beaver is publicly viewable in the so-called "consensus protocol", which fosters the establishment of trust between members (cf. Soska et al. 2016: 1 f.).

These examples highlight the fact that illegal online platforms, their infrastructure and their various mechanisms and procedures are constantly being developed further with the aim of providing their users with even better protection against measures taken by the law enforcement authorities or against attacks by other cybercriminals, and to facilitate trading in illegal goods and make it more efficient (cf. Buxton/Bingham 2015: 16). These efforts to optimise the platforms have an effect on the structure of the platforms and hence also on the interaction between their members. However, they also affect the means law enforcement authorities have at their disposal for detecting and investigating the operations of groups of perpetrators, and thus they constantly present law enforcement with new challenges.

10. Conclusion and need for action

The evaluation of the current state of research into the subject of "Criminal Structures On Illegal Online Platforms" showed that a number of quantitative and qualitative analyses have already dealt with such online platforms. Frequently the focus in these studies was on describing the online black market in general, or individual platforms in terms of the products and services they offered, the earnings achieved by the users, the protagonists (background, motivation, etc.), the money flows, the mechanisms for encryption and for establishing trust, etc. In a small number of the sources, the relationships and the criminal cooperation between the members of a platform represented the central subject matter of investigation. None of the sources evaluated dealt primarily with the use of these online platforms by traditional criminal offline groups of perpetrators and their associated activities.

Many of the sources referred to the high threat potential these illegal online platforms represent: they facilitate and increase the commission of traditional offline criminal offences, and often they make the commission of cybercrime in the narrow sense possible in the first place. They pose a threat in that they provide individual perpetrators and groups of perpetrators with a space equipped with various mechanisms and structures where they can cooperate in a collaborative and trusting environment. Frequently they even serve as a catalyst for the formation of new cybercriminal groups. They foster a subculture that virtually legitimises criminal behaviour and promotes entry into cybercrime by individuals without a criminal background.

Building on a range of different mechanisms, online platforms possess an inherently hierarchical structure within which members can interact in a trusting and professional manner. In this way they structure the cybercriminal activities between various protagonists (cf. Lusthaus 2012: 90). In addition, they increase transparency and in this way help their members make purchase decisions on the basis of a great amount of existing, previously reviewed information (cf. Holt 2013: 166). The existing rules and standards also structure the collaboration between cybercriminals, which may be
network or project-specific in nature, but which may also become more permanent, with new groups being established in the process.

Their use by cyberborn groups or by groups involved in traditional offline Organised Crime was discussed, if only in a few of the sources (cf. Council of Europe 2004, Tropina 2010, UNODC 2013, Europol 2011, Europol 2014, INTERPOL 2016, Lewman 2016). Found even less frequently were findings that were based on empirical data (cf. Bulanova-Hristova et al. 2016, Leukfeldt 2016); even there this subject was not the focus of the study and was only mentioned in passing. It can therefore be concluded that to date the use of illegal online platforms by groups of perpetrators formed offline and online has not been the central subject of an empirical study based on primary data. There is a definite need for more research in this area. Given the relevance of this subject, which is also highlighted by Europol, INTERPOL or the UNODC, among others, it is recommended that efforts be made to close the research gap identified here. Such a study should proceed by building on existing empirical findings, reviewing these systematically and then supplementing them with additional research subjects of relevance. Given that cybercrime is an international phenomenon and that the sphere of influence exerted by groups of Organised Crime is also on an international scale, a study with an international scope would be of particular added value.

The majority of sources evaluated here analysed illegal online platforms for narcotics or for cybercrime tools (incl. services and stolen data). What is missing are comprehensive studies into other areas of crime such as counterfeit money, weapons or human trafficking, and these should be included in a new empirical study.
11. References


