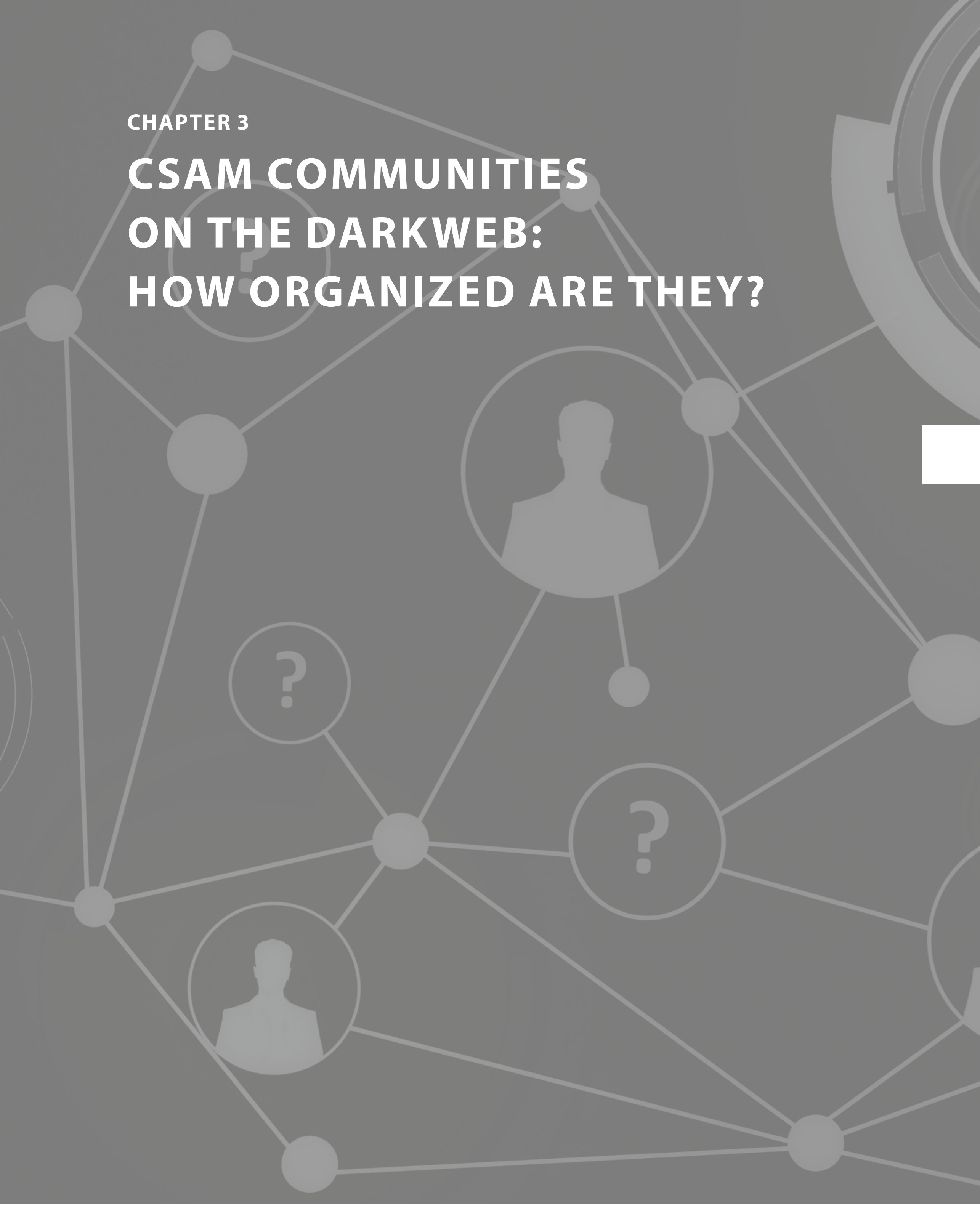
Child sexual abuse material networks on the darkweb: a multi-method approach

Bruggen, M. van der



CHAPTER 3

CSAM COMMUNITIES ON THE DARKWEB: HOW ORGANIZED ARE THEY?

This chapter has been published as:

Van der Bruggen, M., & Blokland, A. (2020). Child sexual exploitation communities on the Darkweb: How organized are they? In M. Weulen Kranenbarg & R. Leukfeldt (Eds.), *Cybercrime in Context* (pp. 259-280). Springer. https://doi.org/10.1007/978-3-030-60527-8_15

Abstract

Because of the growing incidence and increasing technical sophistication of Darkweb child sexual exploitation (CSE), some have begun to label it as organized crime. By itself however, this label adds little to our understanding of the phenomenon. To gain a more detailed insight into the workings of Darkweb CSE, we apply the conceptual framework suggested by Von Lampe (2016) and instead ask: how organized is CSE on the Darkweb? Six police investigation case files were systematically analyzed using methods akin to the Dutch Organized Crime Monitor; complemented with interviews with police officers and public prosecutors. While the barter of CSE material in itself is a deviant exchange, it is embedded in the social network provided by the forum environment. Darkweb CSE requires organization to the extent that running a forum involves a set of interlocking tasks, a certain level of technical sophistication and continued effort to protect the forum from (outside) threats. We conclude that both the CSE crime and the criminals perpetrating it show clear signs of organization. CSE Darkweb fora constitute both associational and entrepreneurial structures that serve the social and criminal needs of their members. In the trust based hierarchy of these networks, keyplayers are able to exert some internal governance. Monetary profit, violence and the desire to monopolize the market however, are largely absent. Detailed insight in the dynamics of Darkweb CSE interactions will contribute more to reducing the harm caused by these crimes than the mere application of a label.

3.1 Introduction

Images of child sexual exploitation (CSE) being bartered through dedicated internet fora are a source of growing concern (Europol, 2018). Many of these fora are now located on the Darkweb: the part of the internet that is not indexed by conventional search engines and only accessible through specific software (such as the TOR webbrowser). Offering users extensive anonymity, the Darkweb provides an ideal platform for such fora to flourish, and for those with a sexual interest in children to access illegal content on a large scale (Finklea, 2017). Recent studies indicate that CSE material constitutes one of the most popular types of content on the Darkweb. While approximately 2% of TOR hidden services are CSE related, approximately 80% of the traffic is directed to CSE websites. Although these percentages might be biased due to bots and DDos attacks being included in these numbers, these figures at the very least indicate that websites hosting child abuse content are frequently requested and visited (Finklea, 2017; Owen & Savage, 2015).

Law enforcement agencies as well as academics have warned about the professional nature and development of CSE crime (e.g. Europol, 2018; Owens et al., 2016). Because of the many actors involved and their high levels of technical sophistication, media, law enforcement as well as academics have begun to characterize Darkweb CSE fora as organized crime (OC) (e.g. Europol, 2018; Jenkins, 2001). In response, law enforcement agencies are currently exploring whether they can formally approach CSE within the legal confines of OC and whether offenders can be prosecuted for OC offenses. Although the gravity of online CSE goes undisputed, characterizing some act as OC based solely on emotion and crime seriousness may obfuscate a detailed understanding of its characteristics and underlying dynamics, and confuse academic and policy definitions (Lavorgna & Sergi, 2016; Leukfeldt et al., 2017; Lusthaus, 2013).

Despite the strong evocative power of labelling some act as OC (Paoli & Vander Beken, 2014, p.878), by itself this dichotomy adds little to our understanding of the phenomenon under scrutiny. When studying crime phenomena, Von Lampe (2016) therefore argues to reframe this question and ask not whether certain criminal actions are OC or not, but rather seek to understand to what extent and in what ways the particular crime is organized. Suggested point of departure is to examine what needs actors involved in the particular crime have, and how the way the crime is organized tends to these needs (Best & Luckenbill, 1980). Von Lampe (2016) goes on to distinguish three types of social structures – entrepreneurial, associational and illegal governance structures that may influence organized criminal activity.

To gain a more detailed insight into the workings of Darkweb CSE, the present study systematically examines data from six large-scale Dutch police investigations into Darkweb CSE fora using the analytical tools previously applied in the Dutch Organized Crime Monitor (Kruisbergen et al., 2018). Building on the conceptual framework suggested by Von Lampe (2016), the overarching research question addressed by the present effort is: how organized is CSE on the Darkweb?

3.1.1 Cyber-facilitated CSE

The evolution of cyber-facilitated CSE is closely tied to the major technological developments that helped shape our current digital environment (Steel et al., 2020). CSE material was first reported being shared on Bulletin Board Systems (BBS) and Usenet newsgroups (Jenkins, 2001). While still limited in the possibilities of sharing other than text content, these newsgroups mirrored current online fora in that they allowed users to post messages and react to messages posted by other users. From the advent of the World Wide Web in 1990, the number of websites dedicated to CSE rapidly increased, with technological progress simultaneously facilitating the exchange of CSE material – both images and videos – in bulk. Raised public and law enforcement attention, and efforts by major search engine providers to block CSE content, appear to have resulted in a gradual decrease in CSE dedicated websites on the open internet in favor of CSE fora on the Darkweb (Steel et al., 2020).

Apart from facilitating the exchange of CSE material, these technological advancements also increasingly provided for opportunities for those with a sexual interest in children to connect with like-minded individuals in numbers hard to realize in real life. Often feeling ostracized from society, to these individuals these online settings generate a sense of belonging, encouraging a positive self-image (O'Halloran & Quayle, 2010). This sense of community is further enhanced by creating an "us versus them" environment – with "them" referring to those unsupportive of child sex (Taylor & Quale, 2003). Based on a content analysis of messages posted on five open internet "child love" fora for instance, Holt and colleagues (2010) found discourses on marginalization (from mainstream society), sexuality (sexual attraction to minors), law (criminalization of adult-child sexual relations), and security (from law enforcement), to structure forum members' subcultural identity. By normalizing adult-child sexual relationships, reinforcing distorted beliefs concerning the consensual nature of these interactions or the lack of harm in watching CSE material, and by "condemning the condemners" (Durkin & Bryant, 1999; O'Halloran & Quayle, 2010), these fora offer settings where virtual communities of people with a sexual interest in children can emerge and grow (Quinn & Forsyth, 2013; Taylor & Quale, 2003). However, as Holt et al. (2010) rightfully note, these findings may not generalize to fora where individuals actually engage in illegal acts – i.c. exchanging CSE material – such as Darknet fora.

3.1.1.1 Darkweb CSE fora

Like fora on the open internet, a Darkweb CSE forum typically lists a number of topics. Below each (sub)topic, strings of "posts" – messages subscribers to the forum can submit – evolve into "threads" representing ongoing online discussion on a certain topic between forum members. On Darkweb CSE fora many topics refer to markers of sexual interest, like age and gender of the child or the nature of the abuse, with underlying threads including links to CSE images meeting this particular sexual preference. Within these threads the most unique, new or popular CSE material is explicitly promoted by accompanying posts, and given more attention through the feedback it receives from members. Usually, members can see an image preview on the forum itself, and then click on a hyperlink that refers them to an image hosting website where the actual content can be viewed and downloaded. Forum subscribers may also publicly discuss their desires in a thread, but proceed to exchange CSE material in online one-on-one contact, for example in private messages on the forum itself, via direct message programs or in an external chatroom. The communication in threads does not stay limited to the negotiations around the exchange of the CSE material, but also includes extensive discussions about for example sexual experiences and desires, (technical) safety measures, law enforcement techniques, and topics like politics and the media. Members can roughly be divided in those that "only" lurk around and use the platform to gain access to CSE material, those that are moderately active and whose posts center around the exchange of the CSE material, and those that are significantly active in the (social) forum community and may even have a formal role in its organization and development. As many fora show CSE images already on their home page and in previews or thumbnails on other forum environments, fora cannot be entered by individuals other than designated law enforcement personnel without committing a criminal offense (Jenkins, 2001).

3.1.2 Entrepreneurial and illegal governance structures

From an economic perspective, Darkweb CSE fora constitute criminal markets where repeated exchanges of illegal goods – i.c. CSE material – take place. Von Lampe (2016, p.101) refers to criminal markets as "entrepreneurial structures"; arrangements of relationships between offenders that enable or facilitate the commission of crime and are geared toward material benefit. Criminal markets resemble legal markets in many respects, but also differ from them in important ways; the illegality of the transaction shaping the needs of market actors and the ways they organize their interactions in response.

The first problem faced by market actors is that of mutual accessibility (Eck, 1995); buyers and sellers need to contact each other. In illegal markets the need for access is counterbalanced by the need for security: the more accessible an actor is, the more he puts himself at risk of being exposed. Depending on the legal framework criminalizing the market, this applies to buyers, sellers or both.[1] Avoiding, or at least limiting, the danger of apprehension constitutes the second problem actors in criminal markets need to solve (Eck, 1995). The third problem is that of allocating value to the exchanged goods, so that the transaction is perceived "fair" by both parties (Beckert & Wehinger, 2013). Criminal markets tend to be characterized by an asymmetric distribution of information favoring the seller. In the absence of government control, buyers in criminal markets need arrangements that prevent them from being duped.

[1] For example, in attempts to regulate the market for commercial sexual services, governments may choose to criminalize only the sex workers, only their customers, or both.

Fourth, like legal market actors, criminal market actors run the risk of victimization by criminals posing either as buyers or sellers, but with no intention of making a mutual exchange (Eck, 1995). In contrast to buyers and sellers of legal goods however, illegal market actors cannot turn to the government to protect their property rights and thus face a need for protection against predatory crime (Varese, 2010). Finally, market suppliers will seek protection against competing suppliers entering or encroaching on their share of the market. In the absence of legal opportunities, competition in criminal markets is often linked to corruption and violence (Beckert & Wehinger, 2013). To some, corruption and violence used in efforts to monopolize a criminal market even are the defining elements of what constitutes OC (Schelling, 1971; Varese, 2010). To the extent that arrangements between illegal market actors serve to protect actors from victimization or otherwise mirror governmental involvement in legal markets, these arrangements, while indirectly tied to entrepreneurial goals, are referred to as illegal governance (Von Lampe, 2016, p.46-47).

Previous studies on offline criminal markets may serve to illustrate arrangements made to address the needs of market participants. A common distinction in offline criminal markets is that between open and closed markets (May & Hough, 2004). In closed markets buyers and sellers contact each other through social network ties. In open markets buyers and sellers meet at places familiar to both buyers and sellers near to where the routine activities concentrate, like train stations or shopping centers (Jacobs, 1999; St. Jean, 2007). Organizing a criminal market through network ties has the advantage that besides access, networks provide security against prosecution, being wronged in the context of a transaction, and victimization by predatory criminals, as parties are either known to each other or are vouched for by mutual acquaintances. When the criminal market is organized through network ties, market activities tend to be geographically spread out (Eck, 1995). The opposite holds for criminal markets organized by routine activities. Open markets tend to be concentrated and stationary, as buyers and sellers lack a social network to communicate their whereabouts. (Eck, 1995). As transactions between unfamiliar actors are more risky – both buyer and seller could be a cop or a criminal – both parties tend to pay attention to verbal and visible clues signaling trustworthiness (Holt et al., 2014). To avoid prosecution, stationary sellers in routine activity criminal markets typically set up camp at places where management is either corrupt or lacking (Eck, 1995). Sellers may also conduct different phases of the transaction at different places, such to obscure the transaction from law enforcement (Johnson & Natarajan, 1995; Piza & Sytsma, 2016). To reduce the risk of victimization, sellers may attempt to screen unknown buyers (Cross, 2000; Jacobs, 1993), or act as their own guardian – for instance by arming themselves (Varese, 2010). Finally, actors in criminal markets may organize themselves or rely on existing criminal groups, like the mafia or a local street gang, to safeguard the criminal market from unwanted competition (Beckert & Wehinger, 2013; Piza & Sytsma, 2016).

The virtual nature of online criminal marketplaces affects some, but not all arrangements market actors may use to meet their needs. Under the veil of anonymity provided by the Darkweb, sellers can advertise their products and buyers can evaluate different sellers reducing the asymmetry in information available to both parties. Consequently, online criminal markets resemble open legal markets more so in this respect than do offline criminal markets (Bakken et al., 2017). In the absence of physical interaction, online criminal markets typically use formalized reputation systems, including seller and buyer ratings based on previous interactions, to reduce the risk of exposure to law enforcement as well as to avoid conflict and victimization following fraudulent or predatory interactions (Holt et al., 2015; Tzanetakis et al., 2016; Van Hout & Bingham, 2014). To further obscure dealings from third parties, the actual transactions in online criminal markets tend to take place outside the direct forum environment, for instance via encrypted instant messenger services (Holt, 2012; Tzanetakis et al., 2016).

Forum administrators and moderators provide some governance over Darkweb criminal markets, for instance by denying access to those accused of fraudulent transactions. Some fora provide their own escrow service to prevent actors from being wronged in market transactions (Holt et al., 2015; Lusthaus, 2013; Van Hout & Bingham, 2014). There are however obvious limits to the level of governance forum administrators and moderators as well as third parties can provide. The absence of geographical boundaries in the online environment combined with the anonymity of the Darkweb not only rule out the use of physical violence as a means of protection against predatory criminals and market competitors alike, it also complicates monopolization of a given criminal market. The absence or at least lack of clear analogies of concepts central to certain characterizations of OC have led some researchers to conclude that cybercrime is not “organized crime” (Lusthaus, 2013).

3.1.3 Associational structures

Associational structures complete the conceptual triptych proposed by Von Lampe (2016, p.158), and fulfill offenders’ social needs, providing them with a sense of bonding and mutual aid. Criminal associational structures differ in their origins and type of membership, yet have in common that membership establishes and reinforces social bonds between members (Hobbs, 2013). Membership of criminal associational structures can be highly ritualized, or more diffuse. Continued interactions with like-minded others provide the individual with a sense of belonging and recognition, as well as with access to suitable co-offenders (Paoli, 2003). As such, associational structures may indirectly facilitate crime by providing a criminogenic moral environment, a criminal convergence setting and a basis of trust among those perceived as in-group. Importantly, trust between actors is needed for them to proceed in criminal market transactions. Associational structures are governed by (un)written codes of conduct that serve to define the structure and safeguard its continued existence. Some of these behavioral rules, like "no snitching", may also directly serve the interests of individual members. Depending on the specific criminal association, the enforcement of associational rules can be highly formalized resulting in quasi-judicial systems that deal with the question whether rules have been violated, and if so, what penalty is appropriate (Von Lampe, 2016b). To the extent that these quasi-judicial systems are applied to non-group members as well, associational structures begin to overlap with illegal governance structures.

Associational structures also exist in online criminal marketplaces, where they are generally based on a mutual (criminal) interest. Members on Darkweb marketplaces for example report about the fora's addictive nature, due to its 24 hour availability and supportive safety net, which leads to a sense of camaraderie and community (Van Hout & Bingham, 2014). On Darkweb drug marketplaces particularly, members tend to identify as responsible drug users, leading to an atmosphere of positive propaganda and normalization of drug use (Van Hout & Bingham, 2013). Members may provide each other with (individual) harm reduction advise (Masson & Bancroft, 2018; Van Hout & Bingham, 2014). Morality, empathy and reciprocity become embedded values inherent to these markets (Masson & Bancroft, 2018).

The same is true for open internet (support) fora for people with pedophilia and peer-to-peer networks in which CSE is shared among communities of people sexually interested in children. Their marginalized position in mainstream society leads members of these fora to sharing their thoughts and desires with like-minded people online and to an explicit exchange of justifications and pro-offending attitudes. Part of the (un)written code of conduct in such networks is to be open-minded and to make an effort to prevent co-members' true identities to be traced. (Durkin & Bryant, 1999; O'Halloran & Quayle, 2010; Prichard et al., 2011).

Associational structures thus facilitate crime by providing members with access to suitable and trusted potential co-offenders. In addition, they scaffold a set of subcultural values that need to be taken into account when analyzing both offline and online criminal communities, as behavior is guided by rational decision making in risk avoidance and management, as well as the felt need to adhere to subcultural norms (Holt, 2012).

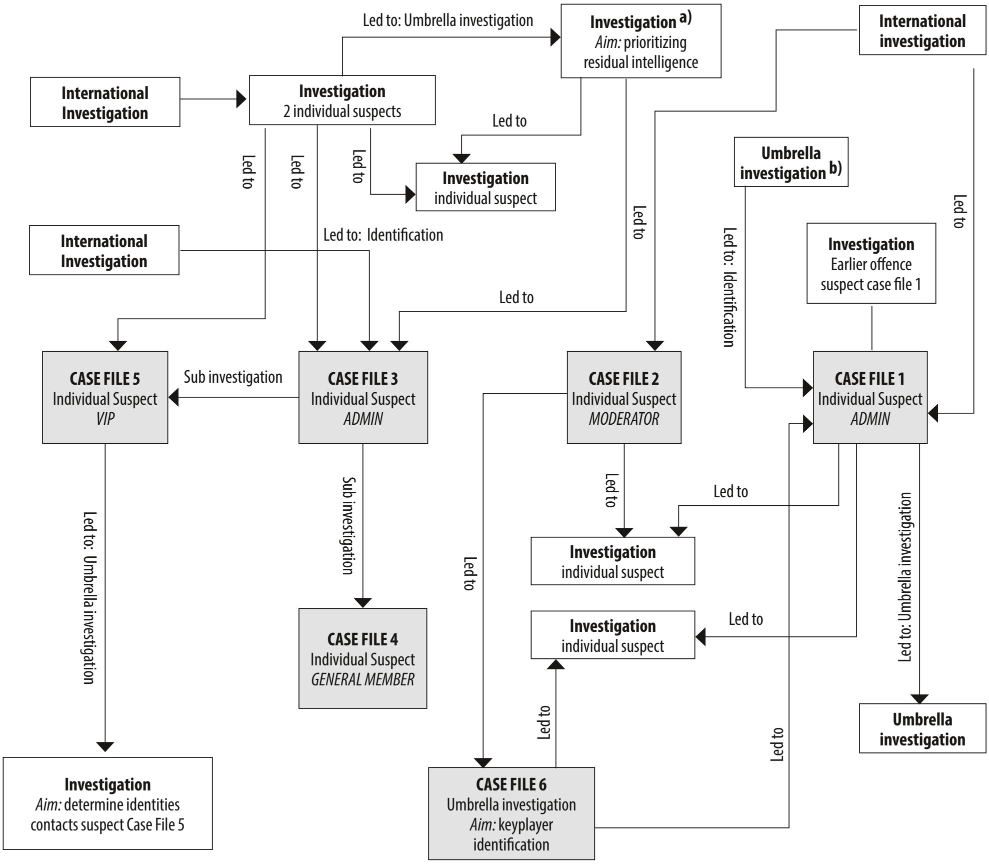
Against the background of what is known about the organization of both offline and online criminal markets, in the current study we address the organization of Darkweb CSE fora as entrepreneurial, illegal governance, as well as associational structures.

3.2 Methods

3.2.1 Sample

In order to gain insight into the organization of Darkweb CSE communities, the complete case files of six extensive police investigations conducted by the National Police of the Netherlands into actors active in Darkweb CSE communities and the criminal activities within these communities were systematically analyzed. The cases included investigations conducted by the national as well as regional police units, and within cybercrime as well as CSE divisions. All cases concerned investigations into a single Dutch suspect, except for case 6, which was an overarching investigation into a group of Dutch Darkweb CSE keyplayers. This case was included because it offered analyses conducted by law enforcement personnel on the structure of fora and the relationships between various suspects. The case files contained detailed suspect-, victim- and witness statements, police observations and analyses, and transcripts of wiretaps. As the investigations involved various police units and sub-investigations, and because national and international Darkweb CSE investigations are often highly interconnected, each case file provided information about many more actors active on Darkweb CSE fora than just the main suspect. Moreover, as most suspects were active on more than one forum, information pertained to eight Darkweb CSE fora that are or were active within the past seven years. Figure 3.1 gives an overview of the cases that were used in the current paper (case files 1 to 6), with their connections to related investigations. As in the Netherlands there is no central or special registration for criminal investigations into Darkweb CSE offenses, for compiling the sample we had to rely on knowledge from law enforcement contacts, and experience of the first author of this paper, who was directly employed with the police. While the sample cannot be taken to be representative of all Darkweb CSE offenders, a deliberate choice was made to include both high ranking members (admins) as well as general members. Permission for the use of the case files for academic research was obtained from the National Public Prosecution Office and the individual (police) team leaders and public prosecutors in charge of each of the investigations.

Figure 3.1 Overview of case files and connections to related investigations



[a] Sometimes within an investigation, extra intelligence is found, which is not further investigated within that particular investigation. This residual intelligence may be collected, and further analyzed within a separate investigation, with the aim of prioritizing which intelligence is most valuable for further investigation.

[b] An umbrella investigation is an investigation not aimed at identifying one specific suspect, but it includes the analysis and intelligence gathering of a group of suspects or a forum as a whole.

3.2.2 Case file analysis

The case files were systematically analyzed using the English translation of the Dutch Organized Crime Monitor checklist (Kruisbergen et al., 2018). This checklist covers key elements of OC including the composition and structure of the criminal group, the ways in which group members cooperate, the nature of the illegal activities they engage in, the modus operandi by which these activities are performed, how group members weigh, manage and avoid opportunities and risks presented to them by their environment, and the criminal revenues gained and how these revenues are laundered

(Kleemans, 2014). The checklist was overlaid and augmented with key characteristics of the criminal structures distinguished by Von Lampe (2016), after which relevant information from the case files was added under the appropriate heading.

3.2.3 Complementary interviews

For each of the six case files, the first author conducted a semi-structured interview with either the coordinating police team leader or the public prosecutor in charge of the investigation. The interviews took place between April-July 2017, and lasted 30-60 minutes. All interviews were conducted prior to the case file analysis, with the goal of gaining an initial insight into the investigations and providing structure to the extensive files. For the interviews, a topic list including the same key elements used for analyzing the case files was used. Because of the sensitive nature of the topic and the researched investigations, the interviews were not recorded, but extensive notes were made and elaborated right after the interviews. Personal information that might link participants to the investigation or that otherwise might compromise their anonymity is not reported.

3.3 Results

3.3.1 Case file descriptions

Table 3.1 summarizes the content of the cases analyzed, characteristics of their main suspects, number of related investigations and identified suspects, and information regarding complementary interviews. This gives a first indication of the web of relationships between (co-)offenders and their activities on Darkweb CSE fora.

Suspects in cases 1 to 3 were administrator or moderator for one or more fora. All had an IT related profession or education, which fits with the advanced technical skills required for running a Darkweb forum. The suspects of cases 1 and 3 were actively involved in the public areas of the fora they were administrator of. Because the suspect of case 2 was moderating a chat environment, his core activities centered around that chat environment. However, at the same time this suspect was in the possession of his own servers and was working on developing his own Darkweb forum. Suspect interviews further indicated that most admins fulfil the administrator role on one forum only, or at least at one forum at a time, as this is a time-consuming and responsible role. Only the suspect of case 1 was the admin of more than one forum. The cases 4 and 5 pertained to suspects with member status only; while they were communicatively active on at least one Darkweb CSE forum, they did not have a role in its development, maintenance or administration. The case files further indicated that apart from sexual crimes against children (i.e. their activities on Darkweb CSE fora, sometimes accompanied with hands-on offenses against children), the suspects often had no criminal record.

Table 3.1 Overview of the analyzed case files

	Case File 1	Case File 2	Case File 3	Case File 4	Case File 5	Case File 6 [a]
Case information						
Investigation year(s)	2018-2019	2016-2017	2014-2015	2014-2015	2014-2015	2017-
Duration investigation	21 months	14 months	15 months	5 months	16 months	unknown
Suspect information						
Age	18-25	30-40	30-40	>60	30-40	n.a.
Gender	Male	Male	Male	Male	Male	n.a.
Profession	IT student	IT related	IT related	Production	Child-care	n.a.
Criminal history	Yes	No	No	Yes	No	n.a.
Activity in number of fora	12	6	1	1	5	n.a.
Duration of CSE activity [b]	6 years	2 years	4 years	2 years	2 years	n.a.
Highest status	Admin on more than 1 forum	Moderator	Admin	General member	VIP	n.a.
Number of contributions [c]	>1,000 public posts + >8,000 images & videos	<50 public posts + 10-20 images & videos + Active private chatter	>3,500 public posts + Active private chatter	0 public contributions + Active private chatter	>700 public posts + >100 images & videos	n.a.
Accusation current case – online offenses	Possession + distribution CP [d]	Possession + distribution CP	Possession + distribution CP	Possession + distribution CP	Possession + distribution CP	n.a.
Accusation current case – offline offenses	hands-on abuse	hands-on abuse	-	-	-	n.a.
Conviction	unknown	5 years prison + hospital order	18 months prison + hospital order (conditional)	10 months prison	15 months prison + hospital order (conditional)	n.a.
Related information						
Information on number of related suspects and identifications	10-20 1 identification	10-20	>20 2 identifications	1	-	10-20 3 identifications
Number of sub-investigations	7	3	6	1	6	0

	Case File 1	Case File 2	Case File 3	Case File 4	Case File 5	Case File 6 [a]
Interview information						
Interviewed person	Police coordinator	Police team leader	Public Prosecutor	Police team leader	Public Prosecutor	Police team leader

[a] This investigation concerns an overarching investigation into a group of Darkweb CSE keyplayers and into a complete Darkweb CSE forum, therefore specific suspect information could not be included in this part of the table.

[b] These figures represent the duration of the suspects' criminal activities according to the evidence as reported in the case files, which may be an under-representation of their actual duration. Some of the suspect interviews indicated that the actual duration of their CSE criminal activity (on the Darkweb as well as open internet) could be up to 20 years.

[c] These figures represent the number of contributions according to reports in the case files, on which the accusation is based. Again, this may be an under-representation of the actual number of contributions.

[d] CP stands for child pornography

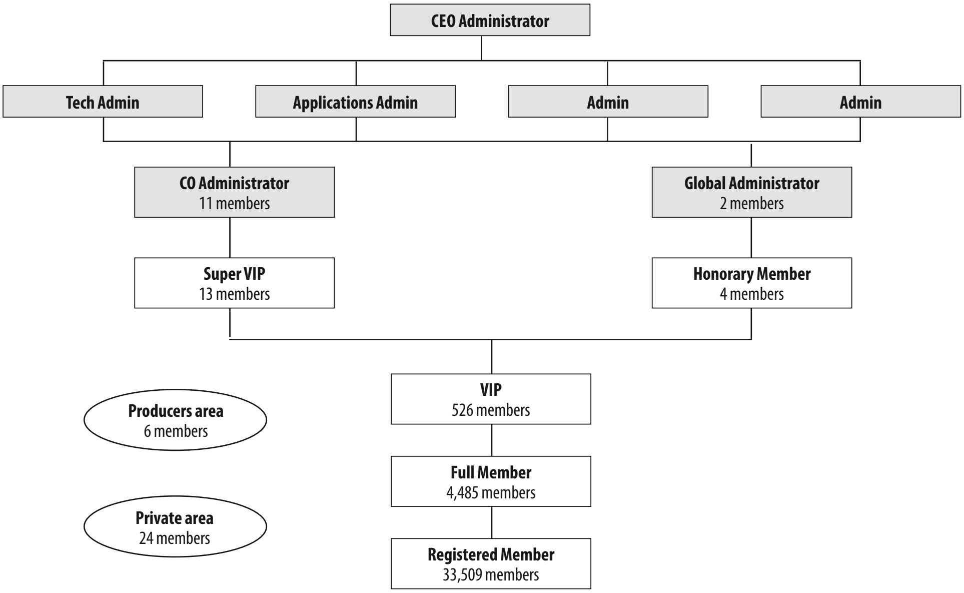
3.3.2 Darkweb CSE fora as criminal marketplaces: Organization and role differentiation

The interviewees describe Darkweb CSE fora as digital marketplaces, in which illegal goods and services are voluntarily offered and exchanged and where there is overlap between suppliers and demanders. By using the Darkweb as the platform for these fora, and by giving members the opportunity to operate under a fictional nickname, the protection of members' identity is practically guaranteed and members are able to engage in illicit transactions in (almost) complete anonymity. During interrogation the suspects stated that while they may use open internet platforms for support and to read about pedophilia, their illegal activity of accessing CSE material stays limited to the Darkweb environments.

Darkweb CSE fora vary in popularity, for example because of the type of material that is being allowed (focusing on "the general child lover" versus "a niche market") and its lay-out and user friendliness. As a result, fora vary in size – from a few thousand up to several hundred thousand of members – and in number of postings. Suspects from cases 4 and 5 voiced explicit preferences for certain fora. The activity of the suspect from case 4 was limited to one forum of his preference solely, and the suspect from case file 5 spent most of his time on one forum of his preference while occasionally checking other fora for new content. Individuals may thus be communicatively active on one forum, and mere "lurkers" on others.

Suspects from cases 1, 2 and 3 further describe a process of step-by-step taking on various organizational tasks and making forum continuation their personal mission. Sustaining a forum and safeguarding it from law enforcement (and hacktivists) requires continued effort of forum administrators. Most of the investigated fora were online and active for several months up to several years. Admins and moderators also make strategic decisions about the forum's organization and focus. The suspect from case 3 described his responsibility of being an administrator as "time-consuming", which left him no time to collect CSE images himself. He sometimes received more unique CSE material from members privately – with the request not to share this further -, as a favor in return to his services to the community. The case files also demonstrate that fora may be structured differently. Whereas case 3 concerned a forum with a "democratic" structure in which various moderators and admins were involved in the decision-making process (see Figure 3.2), in other fora one admin had full decision-making power and only received operational support from others.

Figure 3.2 Organizational chart of an example CSE forum



Note The CEO Administrator is the head administrator of the forum. All other administrators and global moderators are responsible for certain specific tasks or parts of the forum. CO Administrator stands for assisting administrator. VIP members have gained this status by contributing valuable information and content to the forum. Full members have made an approved application, and can access all forum environments (apart from the restricted areas). Registered members have registered, but have not made an approved application (yet). The producers and private areas are invitation-only and restricted, and therefore only accessible to certain forum members.

3.3.3 Entrepreneurial structures

In criminal markets the provision of illegal goods or services typically occurs in exchange for (crypto)currency. This however, does not apply to the Darkweb CSE fora under scrutiny here, where CSE material is the commodity directly bartered without monetary incentives. Case file analysis indicates however that sub-sections of Darkweb CSE fora may exist where financial profit is made. The suspect in case 1 for example spoke about a rumor of a "marketplace sub forum". The interviewees stated that in first instance the most unique or rare CSE material may only be shared or sold in limited VIP groups, before it is exchanged in the wider market. Finally, case file suspects discussed the existence of "studio CSE material", in which children are indecently photographed in professional studios, and from which material is sold to the wider audience. All suspects emphasized that if CSE for monetary gain truly does exist on the Darkweb, this concerns very small sub-communities. No definite proof of actual cash flows through the studied fora was found.

For members of Darkweb CSE fora the absence of monetary motivations mitigates the value problem and the costs of becoming a victim of a fraudulent transaction compared to actors in other (online) criminal markets. The "profit" attached to the distribution of CSE material, is the possibility to gain more unique and new material in return and to acquire a higher forum status. On some fora members get the opportunity to formally thank others for the material they have shared through a "thank you" button, increasing the suppliers' reputation within the community.

Darkweb CSE forum members do however run the risk of exposure by law enforcement. Like actors in other criminal markets, their need for security leads them to screen their transaction partners, and check whether they are "in the know". The interviewees noted that fora have their own "slang" when discussing CSE material. The suspect from case 1 acknowledges that you can never ascertain for 100% that someone can be trusted, but that responding intensively back-and-forth on a particular forum topic with people gives you a good idea of whom you are dealing with. The suspect in case 2 adds to this that he was online 12-14 hours a day, and that he recognized members' writing style, English and typos which fed his believe that he was talking to genuine co-offenders. This is even more so when communicating via personal messages. The suspects describe these as more volatile and quicker ways of communication in contrast to the forum environment where one tends to think longer about messages posted and where one can take the time to write extensive tutorials or other supporting documents. In a substantial part of the CSE transactions, links to CSE images are exchanged not directly through the forum itself, but through one-on-one contact in chatrooms or instant messaging services.

Darkweb CSE fora can be open (e.g. the fora from case file 1), restricted (e.g. the forum from case file 3), or closed. Besides completely open fora – where access is gained by simply creating a nickname and password -, there are fora where active participation, or the provision of child abuse material is required in order to gain access to the contents of the forum. The goal of restricted access is to discourage lurkers, spammers and limit exposure to law enforcement. Some fora have dedicated administrators or moderators who control this access, and determine which potential members do and do not obtain access. The admin from case 3 for example, had the responsibility to control all "permissions" (shared CSE material) from members and to either grand access (green) or no access (red). This process led to a clean and efficient forum environment. Finally, a limited number of Darkweb CSE fora are closed. The location of these fora is not publicly shared on other Darkweb CSE platforms, and a small group of high profile forum members decide who deserves access and to become part the community. Examples of such closed fora are producers-, admins-, or invite only fora (i.e. dedicated fora only accessible for members who can prove that they have produced their own child abusive material, that they are a formal administrator on a forum, or by invitation by other forum members).

The timelines developed by law enforcement analysts in the investigations under scrutiny demonstrate that at one time, there is always more than one CSE Darkweb forum online and active. Some of these fora are clearly connected: although they might have a different focus, they have a significant overlap of members, and the same set-up and house rules. The interviews also demonstrated that technically skilled members often deliver their services to more than one forum at the time. Fora can co-exist within the same timeframe, or they may be initiated sequentially. A reason for this mentioned by interviewees, could be that when a certain forum goes offline, its administrators (and substantial numbers of its members) relocate from this forum to a new one. It seems therefore that administrators form a subgroup in the online CSE community, who are known to each other, and offer their services to various fora sequentially. The suspect from case 1 confirms that although fora operate separately; the broader CSE community is characterized by a high level of interconnectedness. The Darkweb CSE market may therefore best be characterized as a semi-open market, which is in principle open to everyone aware of its location, and able to show that they are part of the "scene". Unlike offline open markets however, network ties among forum members allow for quick communication and relocation in response to outside threats.

3.3.4 Illegal governance

Admins and moderators with forum management responsibilities tend to consider their forum as a business. They speak about their forum in corporate language: fellow members are "colleagues", they have "staff meetings", and they experience stress from having the responsibility of keeping an international forum running (which sometimes needed their attention 24/7). The suspect from case 2 described getting an invitation to a staff meeting two days in advance; the meeting taking place at a separate staff forum. Moreover, staff training took place in a dedicated "command center".

From the case files thus emerges a picture of admins taking on the role of digital place manager. Yet, unlike place managers in offline criminal markets (Eck, 1995), their role in creating, promoting and maintaining a suitable market environment is active rather than passive. As such, they uphold an essential part of the infrastructure of the CSE market, rendering CSE fora something more than mere online offender convergence settings (Leukfeldt, 2015). Admins and moderators make continuous efforts to protect the forum and its members from threats. The admin in case 1 for instance temporarily shut down certain forum functions (portrayal of the (number of) forum members and their online behavior and activity), in order to protect the forum against law enforcement monitoring. The case files also showed that fora are repeatedly attacked by hackers, who for example perform DDoS attacks or spam the website. The administrator from case 1 complained about bots that registered new accounts to the website every few minutes in order to DDoS the forum. He responded by temporarily blocking new member registrations. It was even considered to make the whole forum invite-only.

Internally, admins and moderators set and enforce forum rules, with a major responsibility for members with advanced technical knowledge. Member behavior is continuously controlled to maintain forum efficiency and security. Forum rules and regulations may include the requirement to post topics and posts of a certain content on dedicated and suitable forum areas, the prohibition of sharing identifiable information (within text or images) or use foul language, the requirement to write in English, and may also cover the manner in which illegal content should be uploaded. Admins have the power to determine what formal status and level within the forum's hierarchy members deserve, depending on members' skills and activity. Like in other online criminal markets, the CSE fora's digital environment precludes physical violence in enforcing forum rules. Measures when members fail to adhere to the rules therefore vary from filters that refuse the posting of identifiable content, simple warnings, deletion of a post or all posts of a member, to members being excluded from the forum.

Another important regulative task that administrators and moderators have, concerns the resolution of internal forum conflicts. The suspect of case 1, for instance responded with authority to a forum member who publicly criticized a forum moderator. The admin stated that moderators fulfill this task in their own time and that they are human beings who can make mistakes, especially when they are new on the job, and that people can learn from their mistakes. In his statements he described his role and responsibility of moderator as the person who talks to both sides of the conflict without blaming, and showing the community that the conflict is dealt with. Another example concerns the administrator (case 3), who opened a "warning topic" when he noticed that members were bullying each other. In this forum the emphasis was on community building and friendliness, so action was taken against internal disputes and negative behaviors and atmosphere.

Although all suspects in the sampled cases were active in more than one forum, they tended to describe a certain forum as their "home base", signaling some level of competition between fora. Forum branding and marketing therefore seem points of continued attention. Overall however, the atmosphere appears friendly and cooperative rather than competitive, both within and between fora. Case files 1 and 3 demonstrate that forum administrators even explicitly promote and refer their members to other fora, in order to attract more "customers" and strengthen and improve the online CSE community. As such, the case files provide no evidence for individuals or groups of individuals seeking to monopolize the Darkweb CSE market.

3.3.5 Associational structures

For Darkweb CSE communities, members' shared sexual interest in children is the social tie that binds them. The suspects from cases 2 and 5 emphasize they strongly identify with the shared values of the Darkweb CSE community. They feel that only online they can speak about their deepest sexual feelings and fantasies and that Darkweb CSE fora provide them with the opportunity to show a part of their identity that normally remains hidden. Suspects from cases 3, 4 and 5 note that in the early offending days, they were lone offenders collecting child abusive material from open internet platforms and refraining from communication with co-offenders. Only once they got familiar with the Darkweb, social as well as criminal associations with like-minded co-offenders were formed. The suspect from case 3 refers to the non-judgmental atmosphere on CSE fora. Suspects emphasize the need to extensively write about and discuss their feelings towards children, and the mental difficulties they experience keeping these feelings secret in their offline life. The suspect from case file 3 also mentions that he enjoys the appreciation he receives from forum members in response to doing his task for the CSE community. Some members state that their online activities give them strength to cope with negative feelings experienced in the "real" world. The suspect in case 1 claimed that the feeling of belonging to such a dense social community of friends was so strong, that it led to his return to the community, and his subsequent re-offending, only very shortly after having been arrested and sentenced for possession of CSE material. Although for most members this dynamic is limited to their online life; the suspect from case 5 expressed his wish to also meet with like-minded others in real life.

Darkweb CSE fora each have their own rules of conduct that help define and maintain the forum and directly or indirectly facilitate the ongoing transaction of CSE material. Fora supporting “child love” for example, only accept images in which children seem to “enjoy” the sexual act and do not allow the barter of images that include signs of force or violence. Other fora however, also accept “hardcore” material. Interviewees confirmed that the most extreme fora even accept material that depicts pain and blood. Individuals that fancy violent and sadistic CSE material are repeatedly disliked by those that support “child love”, and appear to be a small minority of the CSE community. The suspects from cases 1 and 2 explicitly state that they are more than willing to help law enforcement to track down people that advocate violence against children. Similarly, exchanging CSE material for monetary gain was not accepted on the fora currently studied. Making money out of CSE was believed to be unsafe and unethical. The interviewees confirmed this notion, and highlighted the communities’ emphasis on generosity, the “free share of something beautiful” and offenders’ aversion to making money out of “child love”. The interviewees added to this that as a response to the increased law enforcement surveillance on the Darkweb, a counter movement of fora that do not accept CSE material at all has arisen. These fora only accept non-sexual and “decent” images of children, and have as their main goal to enable people with a sexual interest in children to speak with like-minded others.

Failure to comply with the forum’s official and social rules can have important (online) consequences. The interviewees explain that there is a lot of “naming and shaming” on Darkweb CSE fora. Case file 1 describes one particular fellow member who is unfriendly, calls people names, manipulates other members and treats them as “slaves”. This results in him being regarded as unpopular and eventually in him being “fired” as forum moderator.

3.4 Discussion

The aim of the current research was to gain insight into the extent and nature of the organization of Darkweb CSE. Using the theoretical framework explicated by Von Lampe (2016), and building on comparisons of Darkweb CSE fora with both offline and online criminal markets, we identified the needs experienced by actors in the CSE market and explored the ways in which actors organize their interaction in response to these needs (Best & Luckenbill, 1980). We find that to a large extent Darkweb CSE fora can be considered criminal marketplaces, as such defining the needs of their members. The absence of financial motives and the limitlessness of the Darkweb environment however, impact both the problems encountered by CSE market actors, as well as their opportunities to organize themselves against these problems in ways that make Darkweb CSE differ from other criminal markets.

Although some variation in open, restricted and closed Darkweb CSE fora was found, balancing between the needs of accessibility and security (Eck, 1995; May & Hough, 2004), the Darkweb CSE fora in the current sample seem best characterized as semi-open markets. Although access to most fora is in principle open to everyone, given the absence of search engines on the Darkweb, one has to know the website's address to be able to access and enter the forum environment. Having entered, potential market participants may be subjected to additional requirements, such as repeated postings and online presence to ensure the legitimacy of the actors' intentions. Like offline criminal markets operating through social networks, Darkweb CSE fora seem able to quickly react to law enforcement intervention by relocating their activities, communicating their new location through the social network underlying the CSE community.

Security is a constant concern for Darkweb CSE market actors. Forum members tend to show caution when entering in CSE transactions with other members, and use verbal cues in attempts to rule out law enforcement infiltration. Establishing and maintaining a Darkweb CSE forum requires time and effort. Forum administrators and moderators act as place managers. Whereas offline criminal markets tend to be established at places where place managers are either absent or corruptible, the role of administrators and moderators of Darkweb CSE fora exceeds that of merely hosting an online offender convergence setting (Leukfeldt, 2015). They also exert governance over forum members, meeting out rewards and punishments for adhering and transgressing forum rules. Administrators and moderators of Darkweb CSE fora thus have an active role in promoting a predictable environment in which market actors can do business.

While commercial CSE might be present on the Darkweb, none of the fora under scrutiny here evidenced crime for monetary profit. An explanation of this may be that the subcultural, validating and assisting atmosphere (Durkin & Bryant, 1999; Jenkins, 2001; O'Halloran & Quayle, 2010) is more important to forum members than a potential for financial gain. Based on the strong moral objections against commercializing CSE that speak from the available data, group norms reiterated through the associational structures of Darkweb CSE fora seem to act as an important barrier. The direct barter of CSE material reduces actors' need for protection against both fraud and predation. This may explain the absence of sophisticated rating systems in Darkweb CSE fora aimed to signal trustworthiness as seen in other licit and illicit online marketplaces (Holt et al., 2015; Tzanetakis et al., 2016; Van Hout & Bingham, 2014).

Finally, based on the fora and suspect interviews in the current sample, the Darkweb CSE community seems to be characterized by an absence of a need for protection from market competitors. Again, Darkweb CSE not being a "crime for profit" in the monetary sense may explain this. While admins and moderators do promote “their” forum, their shared goal is to facilitate and increase access to CSE material. While competing fora may seduce current members to frequent different websites, they also offer access to potentially new and unseen CSE material. Scaffolded by the associational structures these Darkweb CSE fora provide, dedication to a common goal seems to preclude the need to monopolize the market.

The current study was able to use detailed law enforcement data on actors active on different but interlinked CSE fora. As such, it provides a unique window to the Darkweb CSE organization. Two important caveats however deserve mentioning. First, although the data used are unique, we have no way of knowing the extent to which either the CSE offenders or the CSE fora studied here are representative for the Darkweb CSE community as a whole. The suspects within the current sample are caught by law enforcement, which could be due to the fact that they are “organized”, and have contacts and relations with other CSE offenders. It is entirely possibly that “less organized” and interconnected Darkweb CSE offenders are able to avoid law enforcement attention, affecting the generalizability of our results. Likewise, those fora “most organized” in terms of for instance technical sophistication or membership requirements, may also successfully preclude law enforcement detection, and hence be underrepresented. Given the extensive law enforcement investigations to gain insight into these CSE fora, the periods over which suspects were active on them, and the parallels in suspects’ testimonies, we also have little indication that the offenders in the current sample are atypical. Still, we urge researchers to foster collaborations with law enforcement agencies to facilitate future research on the topic. Second, CSE material constituting “absolute contraband” (Von Lampe, 2016), severely limits academic researchers to access these fora themselves. As these fora depict CSE images already on their homepage, researchers would be liable to criminal prosecution just for visiting them. To learn about the organizational structures of Darkweb CSE fora, research methods using these fora’s meta-data, may be of help here. Previous research using network methods for example has shown that much can be learned by studying interaction patterns between forum members, without the need to access the content of these interactions (Fonhof et al., 2018; Westlake et al., 2011).

Growing societal concern about a particular type of crime may trigger the “knee-jerk” reaction of media and policymakers labelling these crimes as OC (Paoli, 2002), as was the case with Darkweb CSE (Europol, 2018; Jenkins, 2001; Owens et al., 2016). Doing so however seems to inevitably evoke an equally “knee-jerk” reaction in academics debating whether this label is appropriately applied, but who have far from reached consensus on what are the concept’s defining elements. Drawing parallels between online and offline criminal markets, we have taken a different approach, and instead have addressed the ways in which actors in the Darkweb CSE market organize their interactions to meet their various needs. Detailed insight in the dynamics of Darkweb CSE interactions will contribute more to reducing the harm caused by these crimes than the mere application or non-application of a label.