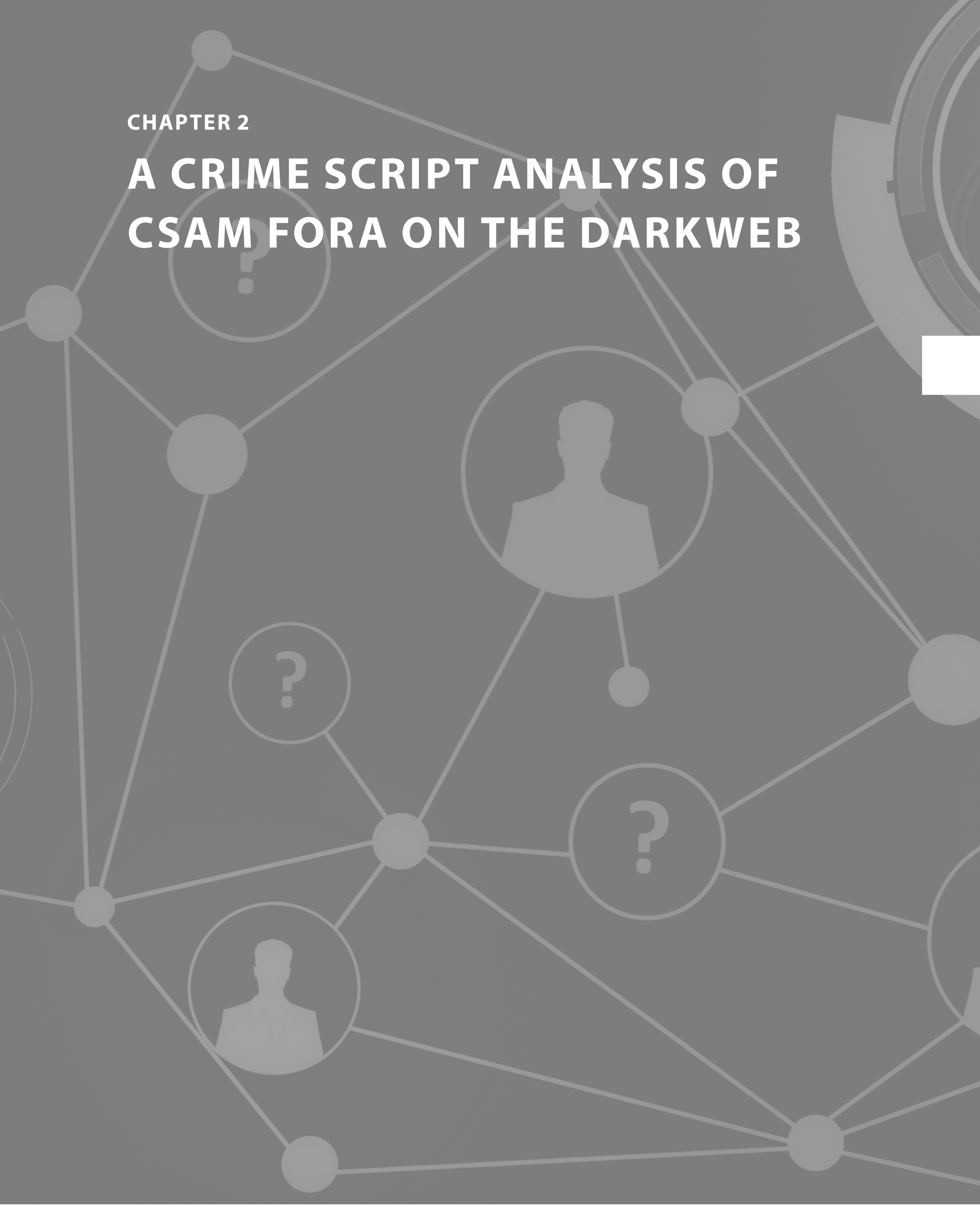

CHAPTER 2

A CRIME SCRIPT ANALYSIS OF CSAM FORA ON THE DARKWEB

This chapter has been published as:

Van der Bruggen, M., & Blokland, A. (2021). A crime script analysis of child sexual exploitation material fora on the Darkweb. *Sexual Abuse, 33*(8), 950-974.
https://doi.org/10.1177/1079063220981063

Abstract

This study's aim is to contribute to the knowledge on the steps involved in child sexual exploitation material (CSEM) crimes committed in Darkweb CSEM communities. Due to the anonymous and illegal nature of these communities, academic research is scarce. This study provides a crime script analysis of member communication data from four CSEM Darkweb fora obtained by law enforcement. For cross-validation, suspect interviews from a relevant case file were analyzed. A step-by-step description of the crime process, starting with the preparations necessary to access Darkweb CSEM fora and ending with the postactivity behaviors of exiting the crime scene and preventing detection, is given, focusing on the casts, activities, probs, and personal and contextual requirements at each stage. The findings highlight the scope of the CSEM problem, as well as the influence the Darkweb has on the way the crime is committed. Suitable targets for law enforcement intervention are discussed.

2.1 Introduction

According to Europol's (2018) internet Organized Crime Threat Assessment, the amount of detected online child-abusive material continues to grow. Project Arachnid, using an automated website crawler to scan over 230 million websites over a 6-week period in 2017, detected over 5.1 million unique webpages that together hosted over 40,000 unique child-abusive images (Canadian Centre for Child Protection, 2018). One of the reasons for these findings is believed to be that, with the introduction and growth of the internet, searching for and getting involved with child sexual exploitation material (CSEM) has become much easier and faster (Frank et al., 2010; Shelton et al., 2016). The possibilities of the internet, however, have not only simplified access to CSEM – pictures and videos can be downloaded in bulk in a split second – they have also drastically changed the way these offenses are committed (Europol, 2017; Holt & Bossler, 2014; Owens et al., 2016).

Before the internet, consumers had to rely on paper copies of magazines containing child-abusive material. These were sold – often, but not always, under the counter – in local sex shops, or obtained directly from the publisher via a surface mail subscription. Producers and consumers of the material were largely separate parties. Law enforcement's awareness of and concern about the issue at the time was scant and their efforts to identify and apprehend offenders limited (Owens et al., 2016). Still, for many consumers, the potential social costs involved when recognized buying child-abusive material still may have fueled a veil of secrecy surrounding CSEM which prevented them from openly interacting in large networks.

With the advent of the internet, however, individuals could now express and pursue their sexual interests online from the privacy of their own homes, safe from the watchful eye of their offline social environment (Rimer, 2017). Popularization of the digital camera furthermore enabled basically anyone willing to produce CSEM themselves. This facilitated the evolution of internet communities where individuals with a sexual interest in children could not only exchange sexual fantasies but also actual abusive material (Europol, 2018; Goodman, 2015; Leukfeldt et al., 2016). Those with an interest in CSEM could now contact like-minded individuals across national borders and easily obtain material from all over the world. The anonymity offered by the internet furthermore allows offenders to develop enduring personal relationships that extend beyond a simple market exchange. CSEM is therefore regarded as a "cyber-enabled" crime in which the new global and network opportunities of the internet are misused to commit already existing forms of crime, but on a much larger scale (Wall, 2007).

Whereas a sizable academic literature pays attention to cyber-enabled sexual abuse (e.g. grooming, or downloading CSEM from the open internet), still little is known about the workings of the most recent and sophisticated CSEM platforms on the Darkweb. This may come as no surprise given that only in recent years law enforcement agencies have become more active in combating this form of crime. Using communication data from four internationally operating CSEM fora seized by law enforcement agencies, this study seeks to shed light on the steps involved in CSEM crimes committed in global communities on the Darkweb.

2.1.1 Studying CSEM communities on the internet

The lack of spatio-temporal constraints and perceived anonymity of the internet have facilitated an unprecedented growth of cybercommunities around countless topics deemed deviant by society at large, including communities accommodating those with a sexual interest in children (Durkin et al., 2006). Online communications between members of such communities have provided researchers with rich sources of data that can be used to explore and analyze the different ways in which these communities affirm and reinforce the interests of their members. An early example of such research is a study by Durkin and Bryant (1999) – revisited by O'Halloran and Quayle (2010) – in which data from an online support forum for persons with a sexual interest in children was used to explore the needs, justifications, pro-offending attitudes, and explanations for members' sexual orientation through content, and thematic analysis of their online communications. Other studies examining such online communities and posts include Holt et al. (2010) and Prichard et al. (2011). One overarching conclusion drawn from these studies is that individuals with sexual feelings toward children often feel marginalized, and fear stigma and negative responses from mainstream society (Grady et al., 2019; Lievesley et al., 2020). For some, this leads to a strong need to share their feelings with like-minded people online. However, given that these communities manifest themselves on the publicly accessible parts of the internet, the Clearnet, those participating in these communities usually refrain from online behaviors that would make them liable to prosecution. Moreover, the majority of Clearnet support fora also explicitly prohibit behavior that is illegal. This limits the relevance of these studies for understanding the process of committing CSEM offenses. An exception concerns the traditional underground bulletin board systems (bbs) and newsgroups, accessible only to the technically skilled, where child-abusive images were believed to be digitally exchanged for the first time (Jenkins, 2001).

This all changed with the rise of the Darkweb, where some of these communities are nowadays located. The Darkweb is the hidden and encrypted part of the internet that is not indexed by conventional web search engines, and that is only accessible through specific software (such as the Tor webbrowser) providing the user extensive anonymity. Despite being originally developed for legitimate military and civilian purposes, because of its anonymity and absence of guardianship, the Darkweb also provides an ideal hosting ground for those involved in illegal activities (Bartlett, 2014; Finklea, 2017; Zulkarnine et al., 2016). Launching of the Tor browser quickly led to the evolution of various illegal online global marketplaces, like the infamous Silk Road, where buyers and sellers of different kinds of illegal goods and services could meet and do business in relative absence of law enforcement surveillance (Martin, 2014).

Those with a sexual interest in children were also quick to transfer their communities to the Darkweb. Here they meet and exchange CSEM via anonymous Darkweb fora and they do so on a large scale (Bartlett, 2014; Europol, 2017; Finklea, 2017; Goodman, 2015; Van Remunt & Van Wilsem, 2016). As at present, the Darkweb has no search engines, the precise address or URL of such a forum still has to be obtained through alternative offline or (open) online social networks or through Darkweb referral websites. Once the address is obtained and the website entered, these CSEM fora closely resemble fora on legitimate topics found on the open internet. For example, like regular fora on the web, CSEM fora consist of various threads. Threads are series of posts – messages forum participants submit to the forum – that relate to specific topics that fall under the forum's general subject matter. On CSEM fora, apart from information regarding other Darkweb CSEM platforms, and technical and securityrelated tutorials, many of these threads also provide links to child-abusive material, commonly divided in age and type categories (Finklea, 2017). Members of these fora post messages and react to messages by others in these threads. Like the cybercommunities on the open internet, such communications between parties participating in these illegal marketplaces provide a vast source of research data. Data that criminologists have only begun to explore (Yip et al., 2013).

CSEM fora differ from other illegal marketplaces in that they usually lack a commercial goal – no crypto currencies are involved – but rather aim to facilitate the barter of child-abusive material among fora members. As access to and possession of these materials is considered criminal by itself, these fora – unlike the aforementioned criminal marketplaces – are off limits to researchers (Jenkins, 2001), and access to these fora can only be acquired through designated law enforcement agencies. Moreover, as law enforcement investigations are extremely challenging and time consuming, as yet, data on these types of crime available for academic research therefore are still scarce. Notwithstanding the public and research interest in online CSEM, these legal difficulties may explain the relative absence of studies focusing on Darkweb CSEM fora.

2.1.2 Current study

The aim of this study is to contribute to the knowledge on the steps involved in the exchange of CSEM in international CSEM communities on the Darkweb. To achieve this aim, this study uses crime scripting as a methodological tool. Crime scripts systematically analyze the crime-commission process using a step-by-step approach, highlighting the sequence of decision points the individual goes through, as well as the resources required at each step to successfully commit the offense (Cornish & Clarke, 2002). Analogous to a film script, for each stage, the crime script identifies the casts, or actors, the actions these casts need to carry out to successfully further the commission of the crime, and the props or "facilitating hardware" they need to have available to do so (Borrion, 2013; Gibson et al., 1980). Crime scripts have been applied to a wide range of individually committed criminal acts, including pickpocketing, burglary, and auto theft (see Dehghanniri & Borrion, 2019 for an overview), but also to more "organized" forms of criminal behaviors involving multiple actors, like drug manufacturing (Chiu et al., 2011), money laundering (Gilmour, 2014), or illegal waste disposal (Tompson & Chainey, 2011). For example, a study by Hutchings and Holt (2015), who used 1,889 posts from 13 online black markets for stolen data, showing that artifacts created by these fora – that is, forum posts – can be used to inform the crime script. Recently, researchers have also begun to use crime scripting to analyze sexual crimes. Beauregard and colleagues (Beauregard et al., 2007; Beauregard & Leclerc, 2007) used both offender interviews and police report data to script the “hunting process” (Beauregard et al., 2007, p. 1069) of serial sex offenders offending against strangers to script serial sex offenders’ search for victims. Based on questionnaire data from a sample of 221 males incarcerated for committing sexual offenses against children, Leclerc et al. (2011) constructed a crime script and designed situational prevention measures for each step in the commission of offline child sexual abuse. Chiu and Leclerc (2017) used crime scripting to examine adult acquaintance rape and to provide situational prevention measures. Building on this prior research, this study uses a crime script approach to systematically analyze the actors, actions, and resources involved in the commission process of accessing and bartering CSEM on the Darkweb.

This study uses law enforcement data obtained from four internationally operating CSEM Darkweb fora consisting of the online communication of the members of these fora. Research into this hidden offender population through unobtrusive means offers the advantage of studying the offenders in their “natural habitat.” Although individuals may restrain themselves and take precautions to avoid identification and stigma, here they display behavior that comes closest to their “natural” behavior – that is, observing these offenders in the surroundings of their own choice, acting the way they would be acting without the researcher being present – thereby shedding unique light on the different steps that constitute the offending process. This in turn will not only increase our understanding of the ways in which these individuals operate, but also has the potential to provide law enforcement agencies with information needed to better combat online child exploitation and act against these online communities in a more effective and efficient manner. Darkweb fora are not publicly available, as beyond access to the TOR Browser, further registration on the (illegal) forum is required. Due to the illegal character of such fora, data regarding communications between forum members are only available for law enforcement officers with special clearance, as researchers would risk participating in illegal behaviors. As were prior studies by Yip et al. (2012, 2013) into illegal carding, this study is therefore primarily based on forum data seizured by the police, emphasizing the importance of researcher–practitioner partnerships in this particular area of research (DeHart et al., 2017; Tompson & Chainey, 2011).

2.2 Method

2.2.1 Data

The data used in this study consisted of samples of posts and thread titles from four English-language CSEM fora that were active on the Darkweb before being closed down and subjected to investigation headed by Dutch law enforcement, in collaboration with Europol, and specialized child exploitation units from other countries such as Australia, the United Kingdom, and the United States. Experts from a Dutch dedicated law enforcement child exploitation unit were consulted in selecting these four fora based on their variety in size, structure, and criminal process. Moreover, law enforcement databases were checked for the availability of sufficient, complete, and recent forum data, and for the potential of a complete set of threads and posts to be taken into consideration for analysis. The very latest versions of the fora available for law enforcement were used in this study.

Data collection and sampling took place in conjunction with a senior software engineer working for Dutch law enforcement's cybercrime division and was conducted in three separate and consecutive steps. The sampling and analysis of descriptive statistics was done using a proprietary tool for forensic data analysis. This was a police inhouse developed software tool to automatically prepare, congregate, structure, and process large amounts of digital data to enable further analysis. First, the comprehensiveness of the data for each forum was checked by creating overviews and visualizations of all forum threads, topics, and titles. Comprehensiveness of the data was measured using the criteria of at least 10,000 posts and members per forum and a minimum of 10 posts per subforum. As a result, only large-scale CSEM fora (rather than smaller subcommunities) characterized by extensive communication were made subject of the current research.

Prior to accessing the data, we discussed with law enforcement experts how to obtain the most reliable and valid sample of posts from the total of nearly 500,000 posts. From studying the fora structures, it became evident that fora are further divided and organized into subfora that can extend into various layers, in which threads center around discussions on certain topics. The expert discussion resulted in the decision to use these subfora to stratify the sample of posts to be analyzed. A sample of all posted messages would likely not have resulted in a full illustration of the proceedings of the forum. As in some subfora the communication is much more voluminous than in others, in an unstratified random sample of all posted messages, data on smaller subfora would have been limited. Even within subfora, threads vary a great deal in length – some may contain only a few posts, others may contain hundreds. Still, steps discussed in these smaller subfora and threads might be equally relevant for the crime script as those discussed in the larger ones.

Initially, samples were taken from the first as well as second layer of each subforum (Table 2.1). However, after a thorough inspection of the data in all samples, it was decided to only use the first layer samples for the analysis. The content of the second layer posts was automatically included within this sampling frame. Moreover, data inspection pointed out that many posts in the second layer were of such length (sometimes exceeding a page) and filled with technical and personal detail that analyzing them would be too time consuming, especially given that these posts would likely add little to posts from the first layer in terms of providing additional information for generating the crime script. To yield a sample encompassing posts on all possible conversation topics, it was therefore decided to use random samples of up to 100 posts per subforum as the basis for analysis. In approximately 25% of the occurrences, the samples consisted of fewer than 100 messages, which indicated that the total number of posts in that particular subforum was lower than 100.

Considering potential ethical and privacy concerns, when applicable, (nick) names of potential victims or perpetrators or other identifiable information was removed from the reported post quotations. Moreover, given restrictions following ethical examination by the National Prosecution Office, communications including explicit sexual language or content of an otherwise sensitive nature (for example, those communications including information on law enforcement techniques) are not reported.

Table 2.1: Descriptive statistics per Darkweb forum in the analysis

Forum characteristic	Forum A	Forum B	Forum C	Forum D
Time span covered in the data	2010–2014	2009–2013	2012–2013	2013
Total number of forum members	105,650	33,130	12,215	14,370
Number of members in administrative team	5	1	1	4[a]
Number of different formal forum statuses	12	3	7	9
Total number of posts	420,000	11,250	32,360	35,500
Number of subfora (first layer)	15	3	20	34
Total number of threads (sample first layer)	1,265	103	603	1,094
Total number of posts (sample first layer)	1,500	103	929	2,373
Number of posts used as additional information in the thematic analysis	15	3	12	6
Number of subfora (second layer)	42	9	52	10
Total number of posts (sample second layer)	3,393	322	3,282	900

[a] These four formal admins consisted of two pairs with the same nickname, which may indicate that in reality there were only two admins on this particular forum.

2.2.2 Case study

Triangulation of the data used to construct the crime script is important to ascertain the script's accuracy and completeness. A police investigation file pertaining to the case of a male in his 30s, suspected and eventually convicted of possessing and distributing CSEM on the Darkweb was used to cross-validate the findings from the Darkweb fora. The investigation file included transcripts of several hours-long police interviews taking place within a timeframe of several months, in which the suspect speaks elaborately about his activities as an administrator (admin) for a large Darkweb CSEM forum in the period 2010 to 2014.

2.2.3 Crime script analysis

Crime script analysis (from now on: CSA) seeks to understand a crime phenomenon by breaking it down into a series of interconnected activities within a rational and goal-oriented crime-commission process (Cornish, 1994). As such, a crime script looks beyond the crime event, and analyzes the full sequence of the crime-commission process, including events leading up to the crime as well as its aftermath. As applied to predatory crime, Cornish (1994) suggests that the crime script can be divided into nine stages: preparation, entry, precondition, instrumental precondition, instrumental initiation, instrumental actualization, doing, postcondition, and exit scenes. Subsequent authors have altered the exact number of stages to fit the crime under scrutiny (e.g. Gilmour, 2014; Leclerc et al., 2011). Following Tompson and Chainey (2011), we prune the initial nine stages of the crime script distinguished by Cornish (1994) to four: preparation, preactivity, activity, and postactivity, and left out scenes of the crime script that deal with traveling to the scene of the crime and selecting and overcoming the victim. This four-stage generic structuring of the crime script fits the nature of the crime under scrutiny here – the online barter of CSEM on Darkweb fora – and has been previously applied to the crimes that do not involve victim selection, such as illegal waste dumping (Tompson & Chainey, 2011) and corruption (Zanella, 2013).

Preparation involves all actions and decisions taken up until the moment of entering the location of the crime, that is, the Darkweb forum. The preactivity stage relates to the steps – both physical and mental – that need to be carried out prior to the criminal activity. The preactivity stage mirrors Cornish's precondition stage and also subsumes target selection, initiation, and continuation, which – given the nature of the crime under scrutiny – are deemed less appropriate, given the absence of direct offender–victim interaction in online CSEM offending. Together, the preparation and preactivity stage make up the crime set up phase (Leclerc et al., 2011). The activity phase refers to the doing or completion of the criminal activity. Finally, the postactivity phase covers Cornish's postcondition and exit stage, and refers to the steps needed to conceal the criminal activity from law enforcement and prevent exposure of the offender. The activity and postactivity stage together form the crime achievement phase (Leclerc et al., 2011).

For each stage of the crime script, we consider the essential casts or actors, activities, the necessary props – or attributes – and personal and contextual requirements (Cornish, 1994). Given that the crime takes place in an online forum environment, we distinguish physical props and personal motivation and capabilities, as well as organizational and environmental factors that are essential for criminal activities on Darkweb CSEM fora. Unlike offline criminal marketplaces that typically make use of locations built for legitimate purposes (Eck, 1995), Darkweb CSEM fora are especially designed and maintained to facilitate criminal behavior. Forum management is therefore an intrinsic part of Darkweb CSEM offending. Nevertheless, not all actively engaged in Darkweb CSEM take part in building and upholding the forum environment. In scripting Darkweb CSEM offending, we therefore distinguish admins and moderators engaged in forum governance from "ordinary" forum members.

Online interactions between forum members are the primary source used to inform the crime script. After initial analysis of part of the data, thread titles turned out to be as informative for the crime script as the content of the individual posts. Because in most instances, thread titles were in fact a summary of its individual posts, they gave a good indication of the content of the conversations. For this reason, the analysis was restarted using only the thread titles from the samples as the units of qualitative analysis. In the case of these being ambiguous or containing insufficient information, thread titles were supplemented with the full content of the post included in the sample (Table 2.1). The length of these posts varied from a few words up to over 1 page. Moreover, when relevant, reference was made to the environment where threads originated.

First, based on a qualitative thematic content analysis (Braun & Clarke, 2006), forum thread titles, some of them complemented with individual posts, were divided into various main themes. The themes were constructed by summarizing the thread titles and posts and represented their shared meaning relating to the various stages in the crime-commission process (preparation, preactivity, activity, and postactivity). Next, themes were grouped under one or more of the four crime script stages, assigning all sampled forum threads to at least one crime script stage. In the next phase of analysis, the content of each stage in the crime script was interpreted making use of a visualization of the full crime process. Finally, vulnerable points for intervention were isolated which are discussed in the final section of this article.

Due to the sensitive and illegal nature of the data, the analysis was conducted by one researcher (the first author), so interrater reliability could not be determined. To ensure that direct consultation with field experts was possible and to build on their knowledge and expertise, data analysis was conducted on the premises of the police's child exploitation unit. To further enhance the reliability and validity of the results, repeated crossvalidation with the case file information and suspect interviews took place.

2.3 Results

2.3.1 Descriptive statistics

Table 2.1 depicts the time span over which data on each of the four fora was available, the total number of forum members, the number of members in the administrative teams of each forum, the number of formal statuses available on each forum, the total number of posts, and the number of subfora on each forum. Examples of formal statuses are: registered member, VIP member, moderator, and admin; referring to the positions of members within the forum's hierarchy. Examples of subfora were pics, vids, boy, girl, hardcore, and softcore; referring to the type and content of the material and information available on that particular part of the forum.

2.3.2 Organizing information on casts, activities, and personal and contextual requirements by crime script stage

The content analysis of the sampled thread titles identified the casts, activities, props, and personal and contextual requirements essential for the completion of the crime process. A summarizing visualization of the intersections of these themes and the four crime script stages is presented in Figure 2.1. Because of the major difference in their role and behavior on the forum, distinction was made between forum admins and general forum members. The following results are organized according to the different stages in the crime script.

Figure 2.1: Intersections of content analysis themes and subsequent crime script stages

Scenes / activities of the crime script (including props)

		preparation	**preactivity**	**activity**	**postactivity**
casts / actors	**members**	• make available a computer in a private space • gain access to the Darkweb • get to know the forum's TOR[A] address • initial motivation to view CSEM[b]	• create nickname • register as a member • gain access to public area of the forum • confirm sexual orientation • neutralize moral objections	• view, download, share CSEM	• shield forum activity • leave forum
	administrators	• find or create hosting location • get TOR address • find technically skilled co-offenders	• offer guidance and tutorials on posting	• offer guidance and tutorials on technical issues • stimulate CSEM conducive environment	• offer guidance and tutorials on security • enforce forum rules • improve forum environment

↓ ↓ ↓ ↓

organizational aspects	• forum marketing	• requirements for gaining full access • membership hierarchy	• organization threads, topics and subfora by content category	• forum branding • forum marketing

[a] TOR stands for The Onion Router, an internet browser giving access to the Darkweb.

[b] CSEM stands for Child Sexual Exploitation Material.

2.3.2.1 Preparation

The preparation phase of the Darkweb CSEM's crime process for admins starts with building a Darkweb forum environment, and for individual members ends with being ready to enter a Darkweb CSEM forum. First, a CSEM forum needs to be built by actors with sophisticated IT skills (personal requirements), and a hosting location (prop) needs to be found. The forum needs to be located on a server, which can be privately hosted or secretly hosted on a server from a third party (hosting provider). Furthermore, a TOR address where the website is located needs to be generated. These prerequisites are supported by information obtained from the case study, where the offender interviews describe the process of finding a suitable hosting location where illegal content can be hosted: "*I hosted the site myself temporarily, but this became infinite as there was no suitable alternative*." Moreover, the interviews describe the search for capable and reliable co-offenders with whom the forum can be built and developed (contextual requirements).

Concerning individual members, actors need to have the necessary props: a private space with a computer with access to the internet and the TOR browser installed. This means that actors have to have basic knowledge of and affinity with the workings of the anonymous internet (personal requirement); something which was previously limited to technically more sophisticated offenders but which is nowadays much more common. Moreover, new members need to know where to go in the first place, so they need to find the TOR address where the forum can be accessed. These conditions are discussed on the forum in threads such as *"How did you discover the* TOR *sites?."* Threads and posts within this section highlighted that most members accessed the TOR fora through a general TOR webpage named *"Topiclinks"* on which CSEM fora are advertised. The hyperlinks of these fora were most often found on Clearnet websites related to CSEM or through personal referral.

Given the effort actors have to make going through this preparation phase, these individuals are assumed to have a certain motivation. Postings from members demonstrate that they may not always be first offenders, as they have been collecting illegal material before, but they are new to the TOR communities: *"new to tor, but long time CP fan"* (where CP stands for "child pornography"). This is supported by the case study, in which the individual in the suspect interviews describes a longtime interest in CSEM, starting in the early 2000s at the open internet, continuing on peer-to-peer networks, and along the way through online contacts getting introduced to Darkweb communities. However, this motivation is not always evident from the start, and many members go through a process and slowly integrate into the community, which becomes evident in threads such as *"thinking of registering"* and *"What's your opinion of me as a […] user?."*

2.3.2.2 Preactivity

The preactivity phase consists of users entering the forum for the first time, by providing a nickname and a password; in other words, actors have to register with a forum account. This means that actors create an online identity, using a nickname that they feel comfortable with or can identify with. When entering the forum, they usually get access to the public areas of the forum and to the environment where the forum's threads, topics, and subfora are introduced. At this stage, it also becomes evident that the forum's leading language is English (confirmed by the case study, where the offender acknowledged exclusively speaking in the English language), though there might be subfora (environments) with a language division, especially meant for members with a certain native language. As giving away your potential native language may help law enforcement in their identification process, these forum sections are less frequently visited. The preactivity stage is thus the stage where actors initially get familiar with the fora's contents, and where they find out where the actual illegal material can be accessed.

In this stage, technical support and advice can be obtained, often in the form of tutorials. Two of the four fora included dedicated sections for "tutorials" and "techzones," where actors could find information regarding encryption, setting up virtual machines, file hosting, safe passwords, and web proxies. These can be recognized by threads such as *"Safety questions for a* TOR *newbie"* and *"How to make thumbnail sheet previews for vids."* The case study illustrates that (higher-ranking) members are responsible for writing these tutorials. On top of the basic computer and TOR skills, these members need to have extended technical knowledge of, for example, programming (languages) and operating systems. Moreover, errors on the forum or on TOR in general can be reported within threads such as *"Tor errors and reporting."*

The preactivity stage is also the stage where, on a personal level, one's potential (sexual) preference for children is confirmed. This might be a reason to continue to explore boundaries, and to decide which legal and illegal actions to further take. In this stage, initial moral objections may need to be diminished as potential users have to decide whether to proceed with the offending process. Sometimes, these issues and dilemmas are explicitly spoken about: *"So I read somewhere that said simply viewing pictures isn't illegal but downloading them is, is that true or just bs?," "Sexual deviant? IDK what I am.,"* and *"Is this ethical?."* Moreover, it is the stage where actors start to get to know each other, visible in threads such as *"What does your username mean?."* Most fora have a dedicated subsection for "introductions" of new members, where one can introduce oneself and get closer to fellow forum members. Members introduce themselves through posts such as *"A little hello from a passionate childpunisher."* An atmosphere open to new members, characterized by a sense of belongingness, becomes visible at this stage. Members welcome each other by sending posts such as *"You are not a sicko brother, you are normal. We are the normal ones the real men and women of the world!!! soon we will rise again and be accepted for the right way of living!," "wot great place! hallo all pedu lovers!"* and *"We have a lot in common, please consider yourself accepted!."* Information originating from the suspect interviews from the case study adds to this that although illegal, the forum is a place for people with pedophilic feelings to come together and that by doing so, at this stage boundaries between the legal and the illegal are quickly becoming blurred. From an organizational perspective, when entering the forum for the first time, actors get introduced to the forum's rules and regulations and with members' status, role division, and the hierarchical order. Where on most fora, the great majority of illegal content can be accessed immediately after initial registration on the forum; sometimes an application with additional requirements needs to be made to be able to access the rest of the forum: "*To apply and access the forum, you need to make here a valid post that satisfies all the posting rules. Please review the 'Application Rules' and the 'How to Post tutorial.'*" According to the case study, these extra requirements are in place to discourage lurkers, spammers, and law enforcement to enter the site and to make sure that members are serious. Members are encouraged to contribute to the forum by posting messages and images, because this is where the continuity of the forum relies on. Through posts such as *"VIP status: what's up with that?,"* and *"Posting a lot of content like this doesn't get members VIP. You can request VIP from the admins, but please PM the admins to do that. Please fix these items so we can approve this post: Please change your title to something more descriptive of what you posted,"* it becomes evident that strict rules are required for members striving for a higher status. The case study demonstrates that to receive a higher status, *"one has to make a personal application for access to the higher-ranking members and one has to be of 'good' behavior."* On some fora, acquiring a higher status or sharing unique or new CSEM can be beneficial, as it may be rewarded by gaining access to special forum areas containing more unique content and visited by other (popular) members of high status. Sometimes, a higher status can only be obtained through personal recommendation and invitation, for example as a sign of appreciation. Members may be motivated to achieve a higher status because of access to more (unique) material or because of a potential increase in reputation.

The most important aspect of the preactivity phase is that actors come closer to committing the illegal act. Once registered, actors can find referrals to illegal material, and the exchange of illegal material is promoted. Often posts within forum topics and threads provide hyperlinks to locations where actors can access illegal material: *"fine links to stories by […]."* This is done in a professional manner, where certain "popular child abuse material series" or types of CSEM are being marketed and praised. Admins point members in the right direction by posts such as *"Welcome to […] We have a wide range of topics around here. All the image forums are labeled with subtext so it will be easy to navigate around."* Referrals to illegal material are also used to present the forum as a whole and to distinguish it from other Darkweb CSEM fora by the type of material that it offers to its members.

2.3.2.3 Activity

The activity stage is the stage of implementation and execution of the illegal act itself (Cornish, 1994; Tompson & Chainey, 2011). On a personal level, during this activity stage, actors consciously make the decision to commit illegal acts. Some forum members even explicitly state this: *"TOR has made me a baby lover."* One reason for doing this, is that they operate in an environment of perceived anonymity, where they trust their fellow members because they are like-minded people. The atmosphere is therefore one of politeness, respect, and recognition: "*Welcome to […] new member/ And thank you for the nice words. I hope you will feel like home here.*" Members are being thanked when they share material, and also members in higher statuses receive a great deal of recognition: *"Just a thanks for all the hard work admin :-)."* The case study confirms this, as the case mentions that personal relationships, respect, and friendly communication are important elements: *"We are a clean board. When I saw that members were bullying each other, I opened a topic in which I told them I would remove them from the forum."* Moreover, taking the time to reply to questions asked by fellow members is greatly appreciated in the community. The atmosphere is one of familiarity; groups of members become online acquaintances. A minor element of competition only comes in where one starts striving for status development, and wanting to become a more important member in the hierarchy. This is supported by the case study, in which the suspect admitted experiencing some jealousy from fellow members after having obtained a higher status.

Actors' personal development happens against the backcloth of an environment where community discussions extend discussions about illegal material. Conversations also include personal experiences and fantasizing, visible in threads such as: *"Kids From Your Childhood You Still Fantasize About,"* "*The best Beastiality and/or CP you ever got to be present and/or participate in*" and *"what's your 'holy grail'?."* Moreover, discussions include societal engagement, politics, and media: *"Human biology & pedophilia," "An Advocacy Group for Pedos?"* and *"Pedos in the news,"* further attesting to a sense of community being present among users of these fora. This is also the stage where potential law enforcement surveillance is explicitly discussed. Because at this stage factual illegal acts are committed, technical shielding is paramount. Often members post messages with questions on how to technically safely commit their crimes: "*Hallo all. I need help with opening rar and 001, 002 7z files in TAILS. I use Tails bat don-t know how open them. Can you please help?"* (TAILS referring to a live operating system aimed at privacy protection and anonymity).

Most importantly, from an organizational perspective, at the activity stage the actual illegal material is accessed, distributed, and commented on through community responses and requests. Environments are organized according to its content, such as "boys," "girls," "softcore," "hardcore," and many other threads or subfora with titles of a more explicit sexual nature. Depending on the focus of the particular forum, content may be more or less extreme, some of them allowing hurtcore (CSEM including violence and images depicting pain) or bestiality material. The variety of the four fora under investigation indicates that there is a variation in forum focus and, consequently, in forum target group. Often thread titles give an indication of the illegal material that can be found: *"9yo girl dances and strips," "boys art photo series," "dog eats boy,"* and, *"pthc 5yo Chinese anal"* (where pthc stands for "pre-teen-hard-core"). Moreover, private requests for material can be done and members comment on the material that has been posted: "*anyone have more of this girl???? Pleeeeeaase.*"

2.3.2.4 Postactivity

The postactivity stage is concerned with all actions that come after the illegal activity, such as the steps necessary for actors leaving the crime scene and for preventing detection (Tompson & Chainey, 2011). Often members are active on a forum for a certain period of time, and in this period, they login to the forum repeatedly. However, members may decide to leave the community for various reasons, for example, out of fear of getting caught, or because of regret. Some members feel obliged to explain when and why they leave the community: *"I am not a frequent poster, more a lurker, but I am an avid reader of these fora. I write to say that changing circumstances mean I shall soon no longer be frequenting these haunts, and while I don't think anyone will miss me, I shall miss all of you. Your stories and discussion have provided much stimulation and enjoyment […] Stay safe and loving,]."* Some members, for security reasons, to assure the community that they have not been arrested, and to prevent others from thinking they are law enforcement, even communicate when they are on temporary leave: *"offline between May,23. To June, 1. vacation."*

New members, on the other hand, continuously enter the forum. From a contextual and organizational perspective, for the forum to survive and the illegal acts to be continued, there needs to be forum and member continuity. Members well connected to the world outside the forum (to either other TOR communities, or to communities outside the Darkweb) can actively attract new members. On the forum itself, other (new) fora are also advertised. There are even dedicated threads where other fora can be advertised: *"other forums?."* When members want to talk personally and in private, they refer each other onto other Darkweb areas such as chat environments: *"Anyone wanna talk to me on torchat?."* According to the case study, the most important decisions about the forum's continuity and other forum management decisions are not made in public, but within private communication between high-ranking members. Moreover, chat environments may be the platform where people easily connect and thus make friends and connections, get to know their way through TOR and get introduced to other members, new fora, and websites.

For the forum to stay “healthy,” admins take care of its (professional) development. Discussions take place about forum improvements, layout, and potential new subfora; sometimes member surveys are even conducted (*“Survey, very brief, please participate”)*. Forum marketing and branding is important. This is demonstrated by a post of an admin: *“Dear fellow mods, it is up to us to make […] known. I will keep you updated here what I do to advertise. Do not worry about informing cops on how to find us. Always assume that the cops are already here (which they are) So be relaxed and […] bring more people onto Tor.”* According to the case study, this also entails advertising the forum TOR address at certain external platforms because members in some way have to get introduced to the forum for the first time. Moreover, admins take care of the enforcement of rights and obligations, and whenever members make mistakes (e.g. when they share potential identifiable information), they will be warned or punished. This fact is verified by threads such as “*members accounts on hold*” and *“Regaining VIP after demotion.”* It is not uncommon to warn members in person through posts such as: “*Hi […] Please do not use the rimg tags anymore as these have been disabled until further notice. Please look at the post made by […], please read now very important.*” The most important aspect in the postactivity stage, that is identifiable in all themes, is for actors to stay away from law enforcement. On a personal level, experiences with law enforcement intervention or previous convictions are discussed. This becomes apparent in threads such as: “*Ever been to prison?*” and “*Ever known anyone who got caught?*.” From a contextual perspective, members advise each other about law enforcement methods that one has to be aware of. This becomes apparent in threads such as: “*Information Security and Anti-Forensics Guide.*” This is the stage where actors are completely aware that they are under law enforcement surveillance – the way law enforcement does this is explicitly discussed in threads such as “*How far can cops go?*” – and that they have to be careful with sharing personal information. Sometimes forum members even suspect active law enforcement intervention: “*WARNING: LEA TRAP SITE.*” For this reason, technical shielding is again very important at this stage. Technical measures are specified to avoid law enforcement intervention. This goes as far as threads as “*Style of Writing Security*,” in which it is explained how actors can write up an English text without giving away their native language through grammar, wording, or expressions. Warnings can also be given with regards to threats other than law enforcement: “*Anonymous at it again – review your security*” and when it is believed that the forum is not safe anymore. However, also at this stage, actors inform each other on how to solve technical problems and how to work with encryption: “*Re: TrueCrypt whole-disk encryption can be cracked!,*” indicating that procedures are in place to prevent detection.

2.3.3 Links to the offline world

The crime scripted in this study and the focus of the Darkweb fora examined is the online access and bartering of CSEM. While not a necessary precondition to this particular sexual crime, numerous threads on the fora under scrutiny refer to possible connections to the physical world and to offline child abuse. Real-world connections with other offenders become visible in threads such as *"Too many risks in meeting other pedos?"* Furthermore, some members are looking for potential locations abroad well known for child prostitution, visible in posts such as *"Is there any list of good fairly recent guides for child prostitution"* and *"Can Thailand still be considered a good pedo destination?."* Some fora have a dedicated environment for such connections; for example, *"looking 4 Hook Up's."* The forum environment that one enters in the preactivity stage also contains discussions that promote or provide tutorage for offline child abuse, visible in threads as *"Practice Child Love"* and *"Ideas on how to access children. For those who don't have their own."* and *"in two weeks my boy will be here – help me planning it!."*

It seems, however, that it is only a small minority of forum members who make these actual connections to the physical world. The forum posts indicate that most connections to other offenders stay limited to the digital environments: "*I wouldn't mind chatting with someone. I am not interested in trading any content or arranging meetups or anything … just talking about common interests or sharing fantasies or past adventures.*" From the case study, it also becomes apparent that there is a large gap between digital and physical abuse and that some members consciously choose to "only" offend online: "*I would never touch a real child, but I do believe that there needs to be a place for people with feelings like mine.*" Moreover, the suspect interviews emphasized the great risks involved in meeting co-offenders in the physical world.

2.4 Discussion

This study aimed to provide a detailed understanding of the criminal activities and processes involved in online CSEM with a specific focus on the workings of CSEM fora on the Darkweb. Using CSA, the casts, actions, and props involved in various scenes of the crime-commission process were identified. Crime script scenes distinguished were *preparation* and *preactivity*, in which actors increasingly ready themselves, both physically and mentally, to commit the offense by getting access to TOR, learning the forum location, registering as a forum member, and neutralizing any remaining moral objections, *activity*, in which CSEM is accessed, downloaded, and/or shared, and *postactivity* which concentrated on efforts to prevent detection by law enforcement.

For each scene, "regular" forum members were differentiated from admins who act as virtual place managers (Eck, 1995), creating and maintaining the online environment in which the crime of CSEM can take place.

This study highlights the scope of the online CSEM problem. At the time of data collection, the four fora analyzed had more than 165,000 registered members, and presumably many more lurkers and visitors still in the preparatory phase of the crime script visiting these TOR websites. At present, the actual number of individuals involved in online CSEM remains unknown, and the fora examined here are in no way meant to be statistically representative of the entire population of persons who have committed an online sexual offense. Hence, no clear statements on whether this offender population is increasing, stable, or decreasing can be made. Jenkins (2001, p.74) loosely estimated the 1999 global population of core users of these fora where criminal acts did take place to be "in the range of fifty to a hundred thousand individuals." The current findings suggest an increasing trend.

The findings also show that the Darkweb has had an unequivocal impact on the way in which the crime is organized. The increased accessibility of the Darkweb combined with its anonymity, has created the opportunity to barter explicit CSEM of dedicated fora in relative impunity and on an unprecedented scale. The organization of these fora reflects "emergent properties of the crime script" (Cornish & Clarke, 2002, p. 52), as it is geared to provide solutions to the challenges individuals need to overcome in each scene of the crime-commission process. Our findings show that, like other Darkweb fora (Hutchings & Holt, 2015), Darkweb CSEM fora extensively tutor their novice visitors in the practicalities involved in preparing for the actual offense. For Darkweb CSEM fora, this tutelage also extends to providing a moral climate in which ethical objections are neutralized and CSEM offending is normalized. Given the strong societal position against sex offenses against children, it seems unlikely that such communities at this large scale could have developed or survived other than in the virtual world of the internet (Jenkins, 2001; Jenkins & Thomas, 2004).

The crime script approach adopted in this study provided the necessary framework to break up the process of committing Darkweb CSEM crime into distinct phases, each characterized by its own obstacles that the script is tailored to overcome (Chiu et al., 2011). Doing so not only provides detailed information on each separate step in the crime-commission process, it also helps to highlight those actions, actors and props crucial to the crime script that are especially vulnerable for law enforcement intervention (Borrion, 2013; Cornish, 1994; Hutchings & Holt, 2015, 2017; Tompson & Chainey, 2011). In this respect, CSA is particularly valuable for complex and new forms of crime characterized by large amounts of information and data (Brayley et al., 2011), like Darkweb CSEM fora.

2.4.1 Implications for practice

The current findings implicate that desirable targets for law enforcement intervention would be the admins and other higher status members of Darkweb CSEM fora. While admins may not account for a disproportionate share in the flow of CSEM through their forum, they do play an important role in maintaining order in the forum's day-to-day interactions, educating members on safety issues, and advertising the forum to potential new members. By safeguarding the forum's workings and continuity, admins and high-status members play a pivotal part in the crime-commission process. Efforts to disrupt admins' workings for the fora could include their physical arrest and also entail technical interventions on Darkweb fora itself. Other suitable targets for intervention are members providing the technical development, support, and security to the fora. Without technical support, shielding, and problem solving, the fora would be much more vulnerable to law enforcement detection and would not be able to exist in a professional manner and for long periods of time. As the technically sophisticated skills necessary to run a large-scale forum are likely to be reserved to only a minority of CSEM offenders, targeting these offenders is expected to have the greatest impact. Removing the less-skilled and adapt members may even lead to the opposite: reducing the member count may lead to a higher efficiency of the remainder members and with that to a better functioning community (Jenkins, 2001).

As it is in crime groups in the physical world (Von Lampe & Johansen, 2004), trust is pivotal to the functioning of CSEM fora. This is especially so during the activity phase, as this is the phase were the actual illegal act is carried out. However, whereas in physical crime offenders have an identity by default and have to work hard to preserve a certain level of anonymity while maintaining trust from fellow offenders, internet offenders start anonymous and create an identity by revealing some personal information to establish trust from fellow offenders. For cybercriminals, their nickname-identity is their reputation and often all that other offenders know about an individual (Lusthaus, 2012). What results is a continuous balancing of creating a trusted identity and becoming well known to other offenders on the one hand, and staying anonymous to hide from law enforcement on the other hand. On the Darkweb fora under scrutiny here, active participation in the forum environment is encouraged as a way of building trust. On a practical and operational level, it is of value for law enforcement professionals to learn about the fora's structures and offenders' actions for future undercover operations where they may have to mirror offenders' language and behavior to achieve a trusted position within the network (Yip et al., 2013). Given the crucial role of trust in criminal networks, law enforcement agencies combatting CSEM on the Darkweb could also focus on preventing offenders to develop trust in the first place, for example, by spreading online rumors, fake messages, or even by hacking the accounts of keyplayers (Yip et al., 2013).

Finally, it is important to note that to survive and thrive, these fora have to actively reach out to potential new members beyond the limits of the forum itself and even beyond the limits of the Darkweb. Venturing outside of the technically assured anonymity of the Darkweb puts these fora, and those that host them, in a position vulnerable to their exposure. The implication of this for law enforcement is that when they face an unidentifiable subject on the Darkweb, traces to their identity may still be found outside the boundaries of the forum itself. Rather than focusing solely on data of the Darkweb fora, it might be beneficial to include other, less anonymous, platforms in the search for an identity of a high-priority suspect.

Results also show that visitors of Darkweb CSEM fora sometimes solicit advice in how to best commit real-world offenses either at home or abroad. This advice includes strategies for finding and isolating victims, and for gaining their trust and cooperation; strategies which previous literature showed to be prominent in crime scripts of the crime-commission process of offline child sex offenders (Leclerc et al., 2011). To the extent that the offenses talked about on the fora are actually carried out, footage of these offenses might subsequently be uploaded and shared among fora members, creating overlap between suppliers and demanders, and perpetuating the flow of new CSEM through these fora. This also indicates that while for some offenders there may be a clear distinction between their online persona – wherein they can escape and offload – and their everyday life (Rimer, 2017); for others, the distinction between the digital and physical environment is much less of a dichotomy. More generally then, law enforcement can use the knowledge of criminal activities and processes obtained through the CSA as background knowledge for further professionalizing and guiding their investigations.

Detailed insight into the workings of Darkweb CSEM fora may have practical implications for treatment providers as well, as it may help them to better understand their clients' activities and motivations. First, knowing each step in the crime script provides the common ground needed for practitioners to speak about clients' online activities. Second, in terms of motivations, for many members, at least those regularly posting, the functionality of these Darkweb fora may extend beyond getting access to CSEM and may also satisfy common desires such as a need for acceptance, a sense of belonging, or even social status.

2.4.2 Research implications

Qualitative research in digital environments brings into life new ethical challenges. First, research involving human research subjects usually requires informed consent. However, informed consent is impossible to acquire in anonymous and closed environments such as CSEM fora on the Darkweb (Markham, 2010). Previous research has considered various ethical and privacy issues when researching digital fora, and researchers have to choose to either participate or to "lurk" and observe forum behavior (Holt, 2010; Rutter & Smith, 2005). Prior research concludes that although informed consent cannot be obtained, the potential harm to individual users is minimized because users are active under a nickname, which means that their true identity remains unknown. Moreover, no direct interaction between the researchers and research subjects takes place. Furthermore, structured and unobtrusive observation of webfora studies subjects in a habitat of their own choosing, and thus does not prompt subjects' (criminal) actions in any way. Still, research and analysis of communities like CSEM fora, may cause the community's behavior to change over time (Holt et al., 2010; Jenkins, 2001). As the subjects under study more than frequently discuss illegal behavior and experiences on these fora, it is possible that when research findings become public, users of these fora experience an increased risk of apprehension, which may activate them to take extra security measures (Hutchings & Holt, 2017). Both the present and previous research however illustrate that subjects are already very much aware of law enforcement presence on these fora (Yip et al., 2013). Nevertheless, users feel anonymous enough to continue their criminal practices.

As such, crime scripting of Darkweb CSEM fora can constitute an important first step toward a more detailed analysis of the various dimensions of members' online behaviors and the underlying communication network, its structure, strengths, and weaknesses by applying methods of longitudinal data analysis (Fortin & Proulx, 2019) and mathematical concepts and techniques from social network analysis (Morselli & Roy, 2008; Tompson & Chainey, 2011). Recently, one such social network analysis was conducted, using one of the datasets that was also used in this study to explore forum structures and identify keyplayers, (Fonhof et al., 2018). Unraveling these CSEM networks in a more quantitative way, identifying keyplayers and brokerage positions, and seeking ways to optimally disrupt these networks so to prevent them from victimizing children remains an important topic of future study (Westlake et al., 2011).

2.4.3 Limitations

Although for this study, there was access to online CSEM fora data that are unique both in nature and in size, a number of limitations should be mentioned. The combination of a large sample of forum data, practical case information and expert knowledge resulting from extensive law enforcement experience of the first author of the study, is considered pivotal for a reliable and valid crime script of CSEM fora on the Darkweb. However, the fact that the analysis of the raw data was conducted by one researcher only, is at the same time a limitation. Although we have sought to minimize single coder bias by elaborately discussing each analytical step with expert law enforcement personnel, the classified nature of the data precluded formal procedures of determining interrater reliability. Further studies finding similar crime scripts as this study would improve confidence in the reliability of our findings.

Since we took CSA as a methodological point of departure, results may have been influenced by the temporal stages of the CSA model chosen (Borrion, 2013; Tompson & Chainey, 2011). An alternative a-priori division in crime script stages might have resulted in variations in the narrative. The available data furthermore only allowed us to script the online barter of CSEM in Darkweb fora. Although links to offline child abuse were noted, our crime script does not detail the offending process by which CSEM bartered on these fora is generated and the possible role the forum community therein. At present, there remain questions to be answered in future research.

In terms of generalizability, the crime script generated likely does not apply to *all* individuals interested in child-abusive material, as the analysis specifically zooms in on the group of offenders active on CSEM fora on the Darkweb; a platform that is not used by all CSEM offenders. Moreover, it is important to remember that, as is indicated by differences between the four fora examined here, not all CSEM fora on the Darkweb share the same structure, level of organization, and focus. For example, some fora are characterized by a generalization of material (all illegal material can be shared), whereas other fora focus on a specific type of material (for example, divided by victim gender or material extremity that is allowed by the forum). Some fora also have more subsections than others, with areas such as "hook ups," separate staff sections, and introduction areas. Furthermore, although all fora had rules regarding safe ways of sharing illegal material to avoid law enforcement attention, these rules differed in how strict they were. The case study added to this that according to the offender's experience, fora differ in their speed and stability. Thus, although these fora all share the same goal, they differ in their ways of achieving this.

The most recent forum data covered in this article are from 2014. There have been, and currently are, many more CSEM fora online – and likely there will be many more in the future – in a virtual environment that is constantly evolving. Moreover, it is very well possible that there are "more inaccessible" fora online, presently outside the view of law enforcement surveillance. This could predominantly be smaller fora, of which chances of exposure given their number of members are limited, but could also disproportionately be larger, more professional, and technically more advanced fora. The generalizability of the current findings must therefore be weighed against the constantly changing technological background. These limitations make that our findings cannot be generalized to other fora without reservations (Holt et al., 2010).

A related issue is that there are likely many members present on the fora, who do not actively participate in communication and who do not exchange illegal material themselves (the so-called lurkers). As the current research is based on communication data, one cannot be sure if the same crime script and personal motivations hold true for those members who like to look around at these websites but knowingly decide not to participate. It is suggested that further research should focus on the crime script and behavior of these lurkers. Even though the case study was selected because of the extensiveness of the investigation and because of the willingness of the offender to cooperate; this intelligence may still suffer from biases or a one-sighted interpretation of the offense under consideration (Brayley et al., 2011).

Finally, as members on the four fora under scrutiny are completely anonymous to the researchers and can only be recognized by their nickname, the possibility that the same individual is active on multiple fora under different aliases, or has multiple registrations on the same forum cannot be determined. Although continuity in the use of nicknames is important in building a trustworthy online reputation, frequently changing nicknames may also be a strategy employed to misguide law enforcement officials. Although there is no indication this is the case in any of the four fora included in the current analysis, as these fora attract members from many different jurisdictions, it cannot be ruled out that part of the behavior observed on the fora is by undercover police agencies in their efforts to make a case against individual members, or even bring down the entire forum under scrutiny. Close collaborations between specialized units from different countries are needed to orchestrate and coordinate such undercover operations to avoid duplication of investigative effort.

2.5 Conclusions

The current analysis provided detailed insight in the steps involved in the process of Darkweb CSEM offending. It showed that the digital age has not only drastically reconfigured the relationship between producers and consumers – blurring this distinction – it also allowed those interested in child sexual abuse to set up communities of a scale unprecedented in the physical world. Within the limits of this study, our exploration of the structure and nature of communications between community members, shows CSEM fora to sustain large, international networks of individuals who take part in some or all activities in the crime script. Given that digital place managers are found crucial to the crime script, our results suggest that to achieve the strongest disturbance of the forum and the crimes committed there, high-status members, including those who offer technical support, should be prime targets of law enforcement intervention.