



Universiteit  
Leiden  
The Netherlands

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

Bruggen, M. van der

### Citation

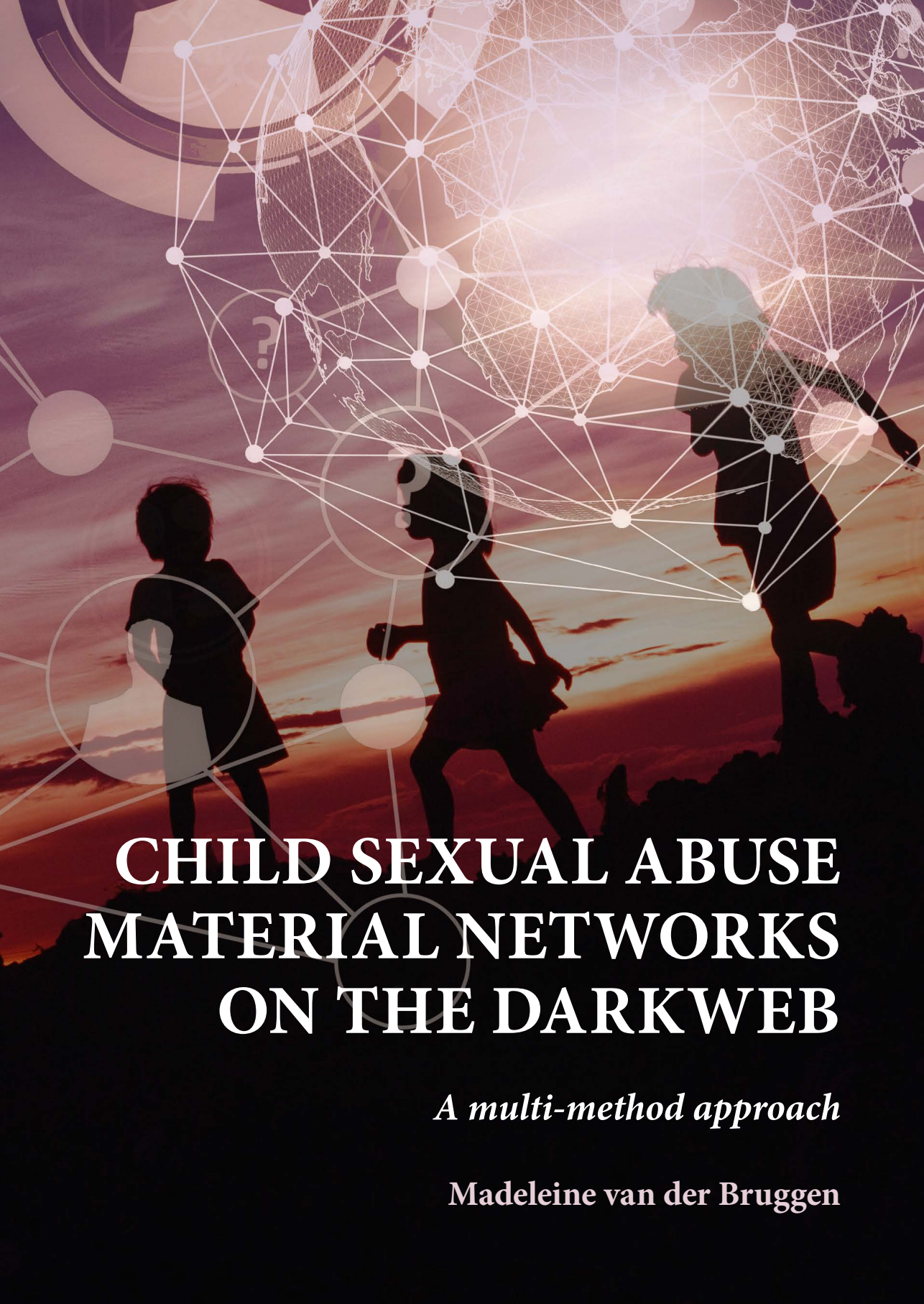
Bruggen, M. van der. (2023, February 22). *Child sexual abuse material networks on the darkweb: a multi-method approach*. Retrieved from <https://hdl.handle.net/1887/3564736>

Version: Publisher's Version

License: [Licence agreement concerning inclusion of doctoral thesis in the Institutional Repository of the University of Leiden](#)

Downloaded from: <https://hdl.handle.net/1887/3564736>

**Note:** To cite this publication please use the final published version (if applicable).



# CHILD SEXUAL ABUSE MATERIAL NETWORKS ON THE DARKWEB

*A multi-method approach*

Madeleine van der Bruggen

## Colophon

© Madeleine van der Bruggen, 2023, Utrecht, the Netherlands

All rights reserved

Contact: [m.van.der.bruggen@nationaalrapporteur.nl](mailto:m.van.der.bruggen@nationaalrapporteur.nl)

Dissertation available from: [www.nationaalrapporteur.nl](http://www.nationaalrapporteur.nl)

Book designer: Studio Kers

ISBN: 978 94 91835 29 2

# CHILD SEXUAL ABUSE MATERIAL NETWORKS ON THE DARKWEB

*A multi-method approach*

Proefschrift  
ter verkrijging van  
de graad van doctor aan de Universiteit Leiden,  
op gezag van rector magnificus prof.dr.ir. H. Bijl,  
volgens besluit van het college voor promoties  
te verdedigen op 22 februari 2023  
klokke 16.15 uur  
door  
Madeleine van der Bruggen  
geboren te Tilburg  
in 1986

Promotor:

Prof.dr.mr. A.A.J. Blokland

Promotiecommissie:

Dr. E.R. Leukfeldt (NCSR & The Hague University of Applied Sciences)

Prof.dr. M.J. van Meeteren (Radboud Universiteit Nijmegen)

Prof.dr. E. Quayle (University of Edinburgh, Scotland)

Prof.dr. M.C. Seto (University of Ottawa, Canada)

Prof.dr.mr. M.J.F. van der Wolf

# ACKNOWLEDGEMENTS / DANKWOORD

Na jarenlang werken, met dit proefschrift als resultaat, ben ik een hoop mensen ontzettend dankbaar. Allereerst gaat mijn dank uit naar mijn promotor, Arjan Blokland. Arjan, ik waardeer het enorm dat je met mij de uitdaging aan wilde gaan, en dat je je samen met mij hebt willen verdiepen in dit heftige onderwerp. Ik ben je erg dankbaar dat je altijd zó betrokken was bij het onderzoek. Je legde de lat hoog, en ik ben trots op het feit dat we alle opgenomen onderzoeken gepubliceerd hebben gekregen.

Ik was überhaupt nooit aan dit proefschrift begonnen, zonder mijn oud-collega's van de Nationale Politie met wie ik werkte aan PIM (Program Identifying Main Targets). Inge van Balen, Arthur van Bunningen en Petra Talens, bedankt voor het fantastische idee om een onderzoeksproject te starten en ons te verdiepen in de wereld van netwerken van seksueel misbruik op het Darkweb. Ik ben ontzettend trots op wat we bereikt hebben, en op het feit dat onze methodiek nog steeds wereldwijd ingezet wordt. Door jullie is het idee van dit proefschrift ontstaan, en daar ben ik jullie ontzettend dankbaar voor.

Ook veel dank aan de verschillende leidinggevers van de Nationale Politie, die mij in staat stelden om aan dit traject te beginnen. Het schrijven van een proefschrift is geen vanzelfsprekendheid binnen de politie, en toch waren jullie bereid om mij hierin te steunen, en mij zelfs 2 dagen in de week te laten werken aan dit onderzoek. Gert Ras, Ben van Mierlo, Dave Jansen, ontzettend bedankt hiervoor! Maar ook andere oud-collega's van de politie (Jesse Donkers, Danny van Althuis, Anoup de Weever) hebben een zeer gewaardeerde bijdrage geleverd door het vormen van een klankbord maar ook door het bieden van gezelligheid en af en toe de nodige borrel.

In 2020 veranderde ik van baan, en ik ben erg blij dat ik dit onderzoek mocht voortzetten in mijn nieuwe functie. In het bijzonder gaat mijn dank uit naar Robbert Hoving en Herman Bolhaar, omdat zij mij binnen de organisatie van de Nationaal Rapporteur de mogelijkheid boden tot het afronden van mijn proefschrift. En daarnaast ook heel veel dank aan alle andere collega's bij de Nationaal Rapporteur. Binnenkomen bij deze organisatie voelde als een warm bad, en ik ben erg blij met jullie constante en welgemeende interesse in mijn project. Ook wanneer ik voor de zoveelste keer klaagde over tijdnood, omdat er nog een artikel naar een journal gestuurd moest worden, én er een monitor deadline aan zat te komen.

Hoewel ik dit proefschrift schreef met slechts één promotor, heb ik me nooit eenzaam gevoeld. En dat komt door de prettige samenwerking met andere auteurs in

een aantal van de onderzoeken. Dank aan Frank Takes, Alain Fonhof, Juliane Kloess, Karlene Clapp, Jessica Owens en (wederom) Inge van Balen, Arthur van Bunningen en Petra Talens. Sommige papers kenden een lange adem, maar ik ben trots dat ze alsnog gepubliceerd zijn! En dank aan stagiaires (Anne Coomans, Anouk Pollman en Vanessa Wijsmuller) voor jullie waardevolle bijdragen aan een aantal onderzoeken.

Daarnaast wil ik mijn familie en vrienden bedanken, omdat jullie mij gelukkig maken en omdat jullie mij altijd ondersteund hebben en hebben willen aanhoren in al die jaren dat ik werkte aan dit proefschrift. Lieve vrienden (jullie weten wie jullie zijn!), ik verheug me op alle borrels, etentjes en feestjes met jullie. En dat ik tijdens die activiteiten niet meer hoeft na te denken over dat proefschrift dat ooit nog een keer af moet. Lieve papa en mama, jullie zijn mijn belangrijkste support geweest tijdens mijn gehele studie- en werkcarrière. Ik vind het zó fijn dat jullie altijd geïnteresseerd in en trots op me zijn. En pap, hier weer een boek van mij dat bij je collectie kan! Lieve Fabienne, lieve zus, ook van jou weet ik dat je trots bent, maar ik ben zéker zo trots op jou. Ook heel veel dank aan jouw vriend Bas en kids Jip en Lieve, voor alle gezelligheid en voor de vrolijke noot zo nu en dan. En tot slot heel veel dank aan mijn lieve man, Remco, die toen wij 4.5 jaar geleden een relatie kregen, dit onderzoeksproject er gratis bij kreeg. Sorry voor alle avonden lang doorwerken, en sorry voor de stress op zijn tijd. Maar vooral heel veel dank voor je geduld en liefde. En dan is het nu tijd om er een punt achter te zetten. Het zit erop!

# CONTENTS

|                                                                                                                                                             |            |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| <b>Chapter 1</b><br>General introduction                                                                                                                    | <b>9</b>   |
| <b>Chapter 2</b><br>A crime script analysis of CSAM fora on the Darkweb                                                                                     | <b>31</b>  |
| <b>Chapter 3</b><br>CSAM communities on the Darkweb: How organized are they?                                                                                | <b>57</b>  |
| <b>Chapter 4</b><br>Profiling Darkweb CSAM forum members using longitudinal posting history data                                                            | <b>79</b>  |
| <b>Chapter 5</b><br>Even “lurkers” download: The behavior and illegal activities of members on a CSAM TOR Hidden Service                                    | <b>113</b> |
| <b>Chapter 6</b><br>Characterizing keyplayers in CSAM networks on the Darkweb                                                                               | <b>131</b> |
| <b>Chapter 7</b><br>Trust and relationship development in Darkweb CSAM networks:<br>A literature review from a psychological and criminological perspective | <b>147</b> |
| <b>Chapter 8</b><br>General discussion and conclusion                                                                                                       | <b>175</b> |
| <b>References</b>                                                                                                                                           | <b>201</b> |
| <b>Summary</b>                                                                                                                                              | <b>219</b> |
| <b>Samenvatting</b>                                                                                                                                         | <b>227</b> |
| <b>Curriculum Vitae</b>                                                                                                                                     | <b>235</b> |



## CHAPTER 1

# GENERAL INTRODUCTION



## Chapter 1: General introduction

Sexual offending on the Darkweb has increasingly gained political and media attention in recent years. International law enforcement organizations detected and shut down various child sexual abuse material (CSAM) websites, or fora, on the Darkweb; operations that were widely discussed in the media. In 2015, the United States, with support from international law enforcement agencies, identified the location of Playpen, one of the largest Darkweb CSAM fora ever known to be online, and arrested the forum's administrator, collected information from other offenders active on the forum, and successfully shut it down. By 2017, the investigation that followed had resulted in hundreds of international arrests and to 55 victims being identified and rescued.<sup>1</sup> At the moment, intelligence gained from this operation still results in international arrests. Also in 2017, Australian undercover agents temporarily took over the management of a CSAM forum in a sting operation to gather evidence on its members; an operation that gained a lot of media attention.<sup>2</sup> Moreover, in May 2021 the German police, in cooperation with Europol and law enforcement authorities from the Netherlands, Sweden, Australia, the United States and Canada, shut down a CSAM forum with over 400,000 registered members and arrested various main suspects.<sup>3</sup> This was not the first time that an international joint operation with a major role for the German police took place; in 2017 the Darkweb forum Elysium was taken down which led to arrests all over the world.<sup>4</sup>

These investigations portray the scope and seriousness of the CSAM problem. Their results are corroborated by recently conducted forum member counts. Web-IQ, a technical company that assists law enforcement with the development of tools to fight online child abuse, counted a total of over two million user registrations across seven CSAM fora, which was estimated to equate to between 300,000 and one million unique users (Web-IQ, 2018). In 2021, over three million accounts were registered across a total of ten Darkweb CSAM fora (WeProtect Global Alliance, 2021). One of these fora hosted approximately 1.3 million child sexual abuse images. Although most of the CSAM exchanged on these Darkweb fora is already existing material that has repeatedly been distributed, sometimes forum members also exchange first-generation material. For instance, in the 24 months after the takedown of Playpen, a Darkweb CSAM forum active between August 2014 and February 2015, 351 sexually abused children were identified and rescued (Raven et al., 2021).

1 <https://www.fbi.gov/news/stories/playpen-creator-sentenced-to-30-years>

2 <https://www.brisbanetimes.com.au/national/queensland/queensland-police-behind-worlds-largest-child-porn-forum-20171007-gywcp.html>

3 <https://www.cityam.com/worlds-biggest-dark-web-child-porn-network-with-400000-members-shut-by-german-prosecutors/>

4 <https://securityaffairs.co/wordpress/60819/deep-web/elysium-website.html>

Beyond these counts and estimations however, empirical knowledge on the workings of Darkweb CSAM fora remains limited. The most important explanation for this is the illegal nature of such fora, complicating data availability for academic research. For the current dissertation however, intensive cooperation with law enforcement resulted in access to various large datasets of different Darkweb CSAM fora. Using these data, the overall objective of this dissertation is to describe and explain the criminal process and offender behavior on CSAM fora on the Darkweb using quantitative as well as a qualitative methods. A more practical aim of this effort is to offer professionals working in the field of law enforcement, offender management and treatment, and child protection a more detailed insight into offenders' *modus operandi*, that can help to design more effective approaches for the identification, detection, assessment and treatment of CSAM offenders. As a result, the analyses in this dissertation are ultimately relevant for the prevention of future offending, and with that for the prevention of future victimization. Hopefully therefore, this dissertation contributes to the protection of children and the reduction of the future number of CSAM victims.

The introduction to this dissertation that follows below, provides the broader context and background of Darkweb CSAM offending.

## **1.1 The transition of crime to online environments**

In many Western countries, crime rates have decreased significantly in the past few decades. Many studies report a drop in the officially recorded crime rates for crime in general (Greenberg, 2014; Griffiths & Norris, 2020; Kim et al., 2015), while some studies also report a decrease for sexual crimes specifically (Bartlett, 2014; CBS, 2021; Wilson & Sandler, 2021). Especially recidivism in sexual offenders seems to have declined substantially in recent years (Caldwell, 2016; Duwe, 2014; Hanson et al., 2018; Wilson & Sandler, 2021). At the same time, the crime rate for online crimes increased (Caneppele & Aebi, 2019). For example, the number of CSAM notifications in the Netherlands in 2019 is five times higher than in 2015, in absolute numbers it went up from approximately 5,000 to 25,000 notifications (Nationaal Rapporteur, 2021). Although not all these notifications lead to an investigation or to a conviction, it does illustrate that crimes being committed online are no longer exceptions.

There are multiple potential explanations for this development, one being that much of the 'traditional' crime has relocated from physical to online environments (Caneppele & Aebi, 2019; Leukfeldt, 2016). It could be hypothesized that some offenders who would have physically offended in the past, are now using the internet for their offences. While this may be true for some sexual offenders, the extant literature finds

that the profiles of physical sexual offenders and that of online CSAM offenders differ significantly and that crossover between both is limited (Babchishin et al., 2015). It is therefore likely that the internet, and more specifically the Darkweb, has made CSAM more accessible to a larger group of (new) offenders. Using large samples of offenders active on Darkweb CSAM fora, for the first time the current dissertation empirically studies the online behavior of this previously hidden population. Studying offenders not (yet) identified by law enforcement in their natural habitat, offers unique insights into their characteristics and behaviors.

## **1.2 The history of CSAM related crime and its transition to online environments and the Darkweb**

Because of the development of the internet and the associated digital opportunities, the crime of the possession and distribution of CSAM has gone through tremendous changes and developments in the previous decennia. The invention and growing possibilities of the hand-held camera, enabling anyone to become a CSAM producer with no need for third-party involvement, led to an increased risk for children of becoming victim of child abuse portrayed on image or video material (Tyler & Stone, 1985). Before the advent of the internet however, there was no digital way of distributing CSAM, so potential viewers had to physically expose themselves and rely on paper magazines secretly – and sometimes even openly – being sold in sex stores, often at a high price (Oerlemans, 2010; Owens et al., 2016; Quayle & Taylor, 2003). Individuals who bought this material in sex shops, or who gave out their personal information when buying material through a mail order organization, had to make an effort to access CSAM and, on top of that, had to take the risk of being exposed.

One can hardly compare this to the time after the commercial rise of the internet and its growing popularity in the general population since the early 1990s, and its further expansion from the early 2000s onwards. Many aspects of the physical life were taken over by the internet through social media and the possibilities of online shopping and studying (Van der Bruggen, 2015; Rogers, 2003). Crime, and the locations where crime is committed, also shifted to online environments. For example, theft can be committed online through the means of stealing online stored confidential information, and financial fraud can be committed online as people increasingly bank online. With crime moving to the online environment, the ‘offender convergence settings’ (Felson, 2003; Felson, 2006) – the places where offenders meet potential collaborators – underlying these crimes also transferred to the internet, and a shift from physical to ‘virtual convergence settings’ took place (Soudijn & Zegers, 2012).

With the growth and increasing popularity of the internet, the exchange and downloading of CSAM through peer-to-peer (P2P) networks became widespread. Examples of such P2P networks are Gnutella, BitTorrent and GigaTribe. It is estimated that approximately 1 to 3% of all P2P search queries are CSAM related (Hughes et al., 2006; Steel, 2009). The key principle of P2P networks is their distributed nature. This means that there is no involvement of a central server with a global overview of the activity in the P2P network as a whole. Instead, users' computers are directly connected through the internet and the exchanges occur directly between peers ('peer-to-peer') (Jarlov et al., 2009). Although the social communication between offenders remained limited on these P2P networks, the emergence of these networks can be seen as the first step from CSAM offenders operating primarily individually, towards them committing crimes in online networks in a semi-anonymous setting on a large scale (Hammond et al., 2009; Hughes et al., 2006; Westlake et al., 2011). Private exchanges were not necessary anymore, as with some basic technical skills, CSAM could now be produced, downloaded and exchanged from a distance with anyone with a computer with an internet connection for free and with some degree of anonymity (Boerman et al., 2017; Leclerc et al., 2021).

Whereas the accessibility of CSAM and the number of offenders involved in it increased, at the same time the societal climate shifted. In its early days, the ideal of the internet was to be a decentralized and independent network free from government intervention (Goldsmith & Wu, 2006; Kleinrock, 2008). Moreover, and especially in the Netherlands, law enforcement intervention was limited because the emphasis was on personal – and sexual – freedom, and governments were deemed not to intervene in private matters. A side effect of these ideals was that it unintentionally cleared the way for people intending to commit illegal acts online, including those seeking access to CSAM (Van der Bruggen, 2015; Leukfeldt, 2016; Westlake et al., 2011). Under pressure of international complaints about the increase of CSAM originating from the Netherlands and under influence of research indicating that the vulnerable position of the child had been ignored thus far, the societal and political opinion started to change. It is therefore not surprising that the societal climate with regard to CSAM offending became harsher, and governments and law enforcement agencies were increasingly expected to intervene and take serious action against people involved with online CSAM. This changing societal climate led to offenders searching for more secure and anonymous ways to commit their crimes. One of the most recent and important developments in the crime of online CSAM is its transition from the Clearnet to the Darkweb. The following paragraphs firstly offer a description of the Darkweb and the way it is used for illegal activities. Next, the currently limited research on Darkweb CSAM will be introduced, together with the research questions that the current dissertation aims to answer.

## 1.3 The Darkweb

With the emergence of the Darkweb, the hidden and encrypted part of the internet, the ease of access and distribution of CSAM developed even further. In order to access the Darkweb, specific software such as The Onion Router (TOR), Invisible Internet Project (I2P) or FreeNet has to be used (Bartlett, 2014; Kaur & Randhawa, 2020; Leclerc et al., 2021; Owen & Savage, 2015). This Darkweb encryption software randomly routes a user's internet traffic through various intermediate servers where repeated encryption takes place, which makes it close to impossible to reproduce the path of the traffic and to decrypt the information. This has the result that the locations of the websites visited and the user's IP address cannot be located, and it significantly reduces the likelihood that a user's online location and behavior can be identified (Weimann, 2016). Moreover, the Darkweb provides 'hidden services': websites that can be recognized by a '.onion' extension, which are only accessible when using the specific webbrowser software (Kaur & Randhawa, 2020; Zulkarnine et al., 2016).

This hidden and anonymous nature of the Darkweb results in an environment of freedom, where freedom of speech, creativity, ideas and information can flourish. Think about the world's most technically savvy individuals who have a platform to further develop their technical ideas and take a leading role in the technical progress of society. Or think about human right activists, journalists or scientists living under oppressive regimes, who can use the Darkweb for access to information and protection from persecution. Unfortunately however, the Darkweb also encourages users to surrender themselves to destructive and sometimes even illegal urges (Bartlett, 2014). Think about political extremists who can use the anonymous Darkweb to express their beliefs and ideas and recruit others. But also think about cybercriminals who can now exploit the Darkweb for their criminal activities. This creates a 'Darkweb dilemma' (Jardine, 2015).

### 1.3.1 Illegal activities on the Darkweb

Often, individuals with illegal intentions explore new technical developments and platforms, such as the Darkweb, at an earlier stage than the general population (Bartlett, 2014). As for the Darkweb, these individuals perceive this as a platform where the risk of detection is low, and where they can operate with greater impunity than on the regular internet (Leclerc et al., 2021). Law enforcement's reaction to new technical developments is often a bit slower, giving offenders a head start, and a fair deal of freedom in creating new and innovating existing illegal activities.

There is some debate about the proportion of legal and illegal content on the Darkweb. This is due to the fact that a clear-cut legal-illegal classification is difficult given

discrepancies between legal frameworks and jurisdictions across the world. Moreover, there is a lot of content that could be considered as occupying a 'grey area'; while its morality is questionable, its illegality is hard to determine (Owen & Savage, 2016). To at least give an indication of the purposes the Darkweb is used for, in recent years academics as well as private parties have developed automatic tools and webcrawlers to crawl the Darkweb, along with dashboards that visualize the content accessible on it (e.g. Ghosh et al., 2017; Pannu et al., 2019; Schäfer et al., 2019; Zulkarnine et al., 2016). Methods such as the social network analysis are then used to determine the links between Darkweb websites and topics and their popularity (Alharbi et al., 2021).

Recent studies indicate that the Darkweb is the part of the internet that is often used for illegal activity. For example, the platform is used for activities related to drug trafficking; think about (former) hidden services such as Silk Road, Agora and Alpha Bay, huge online marketplaces where vendors and buyers from all over the world advertised and ordered all types of drugs. Other crimes the Darkweb is used for, include extremism and terrorism, hitman hiring, hacking and fraud services, phishing and scams, and CSAM (Goodman, 2015; Kaur & Randhawa, 2020; Zulkarnine et al., 2016). The great advantage of the use of the Darkweb for illegal purposes is not only its anonymity, but also the absence of violence, and the ease and safety of sales and purchases because of the fact that the supply chain is short. Some authors expect that the accessibility of illicit products on the Darkweb may lead to increases in the number of consumers of these illicit products (Liggett et al., 2020).

### **1.3.2 The criminal process and organization of CSAM on the Darkweb**

The crime of CSAM committed on the Darkweb is becoming more common and visible, and growing numbers of offenders gather at dedicated Darkweb CSAM fora. Unlike P2P networks, CSAM Darkweb fora have a sole focus on child abuse, which means that these websites are used for this purpose only. These fora are popular and attract a lot of traffic and visitors. Owen and Savage (2015) collected data from TOR hidden services for six months and found that while approximately 2% of TOR hidden service websites are CSAM-related, estimates are that roughly 80% of TOR hidden service queries and traffic can be linked to CSAM. This underlines the urgent need to learn more about the characteristics of Darkweb CSAM fora and the offenders active on them.

The limited information about Darkweb CSAM fora that is publicly available originates mainly from law enforcement reports. These reports describe CSAM fora as similar to legal fora about mundane topics. Communication occurs through 'threads': series of posts or messages centered around a certain topic. Members can post a statement or question under the general heading of the forum, to which other members can respond. In this publicly accessible area, discussions take place, and knowledge

and CSAM is shared (Europol, 2017; Goodman, 2015; Huikuri, 2021). The reports indicate that offenders communicate extensively on these fora. Darkweb CSAM fora are not only used to exchange material – like P2P networks – but also to get in contact with co-offenders, to share fantasies and to acquire new knowledge and skills with regards to connecting with minors and child abuse (Europol, 2017; Goodman, 2015; Kokolaki et al., 2020; Web-IQ, 2018). This seems to indicate that not only does the Darkweb offer a new platform, the use of this platform has led to a change in the way CSAM crime is committed. This leads to the question: how can the criminal process of Darkweb CSAM fora be characterized? Using forum member communication data directly derived from Darkweb CSAM fora, Chapter 2 describes the results of an in-depth qualitative analysis that structurally and step-by-step describes exactly this criminal process.

The currently available public information further shows that CSAM crime committed on the Darkweb is characterized by a focus on security and the use of identity protection technologies. Members frequently inform each other about techniques regarding computer and communication security (Europol, 2017; Goodman, 2015; Wijismuller, 2021). Examples of this are the use of encryption, proxy servers, virtual private networks, fake identities and dedicated computers (Balfe et al., 2015; Holt et al., 2010). More specifically, an often discussed topic on fora is how to cover your identity in order not to be exposed (Kokolaki et al., 2020). Another way in which fora aim to enhance security, is by incorporating a strict forum member hierarchy, depending on the knowledge, activity and contribution of a member and the type of material uploaded. With this status come certain rights and obligations. This means that the forum areas where the most sensitive information and the material of the more violent or unique nature are being shared, is restricted to a limited group of members with a high forum status (Europol, 2017; Huikuri, 2021; Raven et al., 2021; Woodhams et al., 2021). The daily management and technical maintenance of the forum is often the responsibility of the most high-ranking members, the moderators and administrators. These findings lead to a second question: how organized is the crime of CSAM on the Darkweb? And what does this organization look like? Using the theoretical perspective on organized crime developed by Von Lampe (2016), these questions will be explored in Chapter 3.

### **1.3.3 Offenders on Darkweb CSAM fora**

Apart from the criminal process and organization of Darkweb CSAM fora, the question is what characterizes the offenders active on these platforms. Only few and very recent studies have explored what type of offenders access the Darkweb for CSAM and what motivates them. Woodhams and colleagues (2021) analyzed the naturally occur-

ring communication data of 53 anonymous offenders active on the Darkweb in order to investigate the characteristics and behaviors of these individuals. Moreover, in an innovative Finnish project, Protect Children, surveys were launched on the Darkweb in order to gather unprecedented data about the habits, thoughts, feelings, and behaviors of individuals who use CSAM, resulting in a report discussing the findings of the first 8,484 responses (Insoll et al., 2021). These studies give novel insights into the demand side of Darkweb CSAM offending.

Offenders active on the Darkweb are mostly men, who often have a self-reported sexual interest in children, which is sometimes accompanied by other deviant sexual interests, such as sadism, bestiality or urination (Woodhams et al., 2021). The sample that was part of the study by Insoll and colleagues (2021) most often viewed CSAM related to girls 4-13 years (45%), followed by violent or sadistic and brutal material (24%), CSAM related to boys 4-13 years (18%), to infants and toddlers aged 0-3 years (6%), and related to other violent material (7%). The reported reasons for using the Darkweb vary, but include accessing and communicating about CSAM and talking with like-minded others (Woodhams et al., 2021). Approximately half of the participants of the study by Insoll et al. (2021) is in direct contact with other CSAM users.

Alarmingly, the study by Insoll et al. (2021) finds that many users have a first time exposure to CSAM at a very young age: 70% of respondents saw CSAM for the first time when they were under 18, and 39% was even under the age of 13. Reasons for this early exposure vary. A first reason is that some youths expose themselves voluntarily to CSAM because of curiosity. Second, sometimes exposure occurs as part of one's own sexual abuse or exploitation, when an individual for example has a need to understand the abuse or find material depicting their own abuse later in life. Finally, some youngsters may start with viewing legal pornography and become desensitized, which is why they begin searching for the more extreme material. In general, the very first exposure to CSAM occurs accidentally, rather than by deliberately accessing it. Another worrisome finding from this survey is that many respondents are at high risk of contacting children themselves: 52% was afraid that viewing CSAM would lead to physical offenses against a child, 44% said that viewing CSAM made them think about seeking contact, and 37% already had sought contact with a child after viewing CSAM (Insoll et al., 2021). On the positive side, half of the respondents of the online survey expressed that they had a wish to stop searching for and viewing CSAM, and the majority (62%) had attempted to stop for a while but at some point failed (Insoll et al., 2021).

These studies seem to imply that some Darkweb CSAM offenders may initially be motivated by for example curiosity, boredom, escapism or frustration, but then slowly become more engaged with the material. This particular offender group may be motivated to stop offending, but struggle with actually doing so. On the other hand,

there may be a smaller offender group with pedophilic preferences motivated to stay involved with the community and climb its hierarchical ladder. These keyplayer offenders will most likely be less willing to desist (Lanning, 1986; Wijsmuller, 2021).

Given that only a few studies have examined the behavior of Darkweb CSAM forum members, any conclusions drawn from them are still premature. Adding to the empirical knowledge base on CSAM offenders, Chapter 4 and 5 empirically explore which offender profiles and behavioral patterns can be distinguished among Darkweb CSAM forum members. Additionally, Chapter 6 explores whether keyplayers in Darkweb CSAM fora can be identified. Employing various innovative quantitative methods, again using forum member communication data, taken together these chapters provide a first attempt to empirically differentiate various types of forum members and to distinguish keyplayers from general members based on their forum behavior and activity. Distinguishing different types of CSAM forum members is relevant, because law enforcement agencies have to prioritize their investigations when dealing with fora with ten- or even hundreds of thousand forum members.

### **1.3.4 Consequences of CSAM relocating to the Darkweb**

It has become evident that while the phenomenon of CSAM crime is not new, the fact that it nowadays occurs on anonymous platforms like the Darkweb, impacted the way these crimes are committed and how they should be understood. Whereas in the early days of the Darkweb mostly the technically savvy individuals would be able to access it for CSAM, extant research indicates that more recently the Darkweb has become accessible to a much broader and growing population (Europol, 2016; Van der Bruggen, 2018; Wijsmuller, 2021; Woodhams et al., 2021).

Research also indicates that increasing numbers of CSAM images and videos are downloaded and exchanged, including more extreme and unique material (Goodman, 2015; Woodhams et al., 2021). To give an idea, in 2007 the Interpol database in which all known CSAM is collected contained 500,000 unique images. In 2019, that same database contained over 1.5 million images. Moreover, in recent years international law enforcement agencies have seen a major rise in the number of CSAM offenders communicating on the Darkweb (Boerman et al., 2017; Europol, 2016; Europol, 2017; Goodman, 2015; Von Lampe, 2016; Zulkarnine et al., 2016). This increase in offender involvement and the growing demand for new material, means that children are not only increasingly at risk of becoming a victim of sexual abuse, but also of this abuse being recorded and exchanged online.

A further consequence of the anonymous Darkweb is that it has offered a comfortable platform for a group of marginalized people to form communities, and to meet and communicate in a safe way (Huikuri, 2021; Owens et al., 2016; Rimer, 2017).

This group has a sexual interest that is one of the greatest taboos that exist in present day society, which for some of them leads to a need to connect with like-minded people (Bartlett, 2014). Rather than constituting a relatively simple ‘chain of supply and demand’, the exchange of CSAM nowadays takes place in dense social communities, where fantasizing about child sexual abuse is everyday business. Offenders get to know each other and some of them develop long lasting and trusting relationships (Boerman et al., 2017; Goodman, 2015; Holt et al., 2010; Prichard et al., 2011; Westlake & Bouchard, 2016). This leads to the question: how are these relationships and trust between members of Darkweb CSAM fora established? The social nature of Darkweb CSAM communities, and the establishment of trust will be explored from a criminological as well as psychological perspective in Chapter 7 of this dissertation.

These recent developments in the access to and the distribution of CSAM have resulted in a growing public outrage and in governments taking more responsibility in combatting online CSAM (Bartlett, 2014; Shelton et al., 2016), and in many countries law enforcement agencies have increased their capacity to fight online CSAM. While the emphasis of law enforcement efforts is often still on identifying individual victims and individual offenders, there is an increasing focus on identifying and disrupting large-scale CSAM fora and their keyplayer offenders (Boerman et al., 2017; Raven et al., 2021; Shelton et al., 2016; Zulkarnine et al., 2016). Based on the findings of the empirical research reported, this dissertation will end with offering suggestions for law enforcement intervention, and discuss avenues of future research.

## **1.4 Terminology and definition**

To keep ambiguity to a minimum, the most important terms and constructs as they are used in this dissertation will be defined here.

### **1.4.1 Child sexual abuse material (CSAM)**

There are varying definitions for the term child sexual abuse material (CSAM), depending on legal frameworks and on what is proscribed in terms of the age of the victim, and the nature and format of the material (ICMEC, 2018; Krone et al., 2020). This dissertation ignores these definitional discussions, and instead emphasizes the core elements or requirements taken from the Convention on Cybercrime.<sup>5</sup> CSAM is in this regard defined as any material depicting sexually explicit activities involving a child,

---

<sup>5</sup> This convention is also known as the Budapest Convention: <https://www.coe.int/en/web/cybercrime/the-budapest-convention>

or a person appearing to be a child (ICMEC, 2018; Krone et al., 2020). Visual depictions include for example images and videos, but also digital or computer generated images that are indistinguishable from an actual child.

The term CSAM is preferred over the term 'child pornography' (which is the legal term in some countries), because sexualized material that represents children is a form of child sexual abuse, and should not be described as 'pornography' as this term implies consent and carries in it a risk of normalizing the sexual abuse of children and thereby undermining the seriousness of child abuse (Interagency Working Group, 2016). CSAM better reflects the reality of the crime and the impact that it has on and the suffering it causes to victims. At several points in this dissertation the old term 'child pornography' is still used, because these chapters were written when the new terminology guidelines were not yet widely used. Other terms that may occur in this dissertation, and that are used interchangeably with the term CSAM are child sexual exploitation material (CSEM), child sexual exploitation and abuse material (CSEA material) and child sexual abuse imagery.

#### **1.4.2 Darkweb**

The Darkweb is the hidden and encrypted part of the internet, only accessible using specific software, such as the TOR webbrowser (Bartlett, 2014; Kaur & Randhawa, 2020; Leclerc et al., 2021; Owen & Savage, 2015). Other terms that may occur in this dissertation, and that are used interchangeably with the term Darkweb are Dark Web, Darknet and Dark Net.

The Darkweb should not be confused with the Deepweb. The latter contains webpages on the normal internet that are not indexed by web search engines, because these pages are password protected. Examples of this are e-mail accounts, cloud environments, and websites where individuals access their medical or financial information. The Deepweb is, in other words, merely located below the surface, and to access the Deepweb no special webbrowser is needed. The Deepweb accounts for approximately 90% of all websites.

#### **1.4.3 CSAM forum**

On the Darkweb, CSAM is exchanged on various locations and in various ways, but the focus of this dissertation is on CSAM fora (in some papers that are part of this dissertation the term forums is also used): online discussion websites where people can exchange content and hold conversations in the form of posted messages. These Darkweb websites are also called 'CSAM hidden services': websites that can be recognized by a 'onion' extension, which are only accessible when using specific webbrowser software (Kaur & Randhawa, 2020; Zulkarnine et al., 2016). CSAM fora and the accom-

panying ‘hidden services’ are the appearances of the broader and more general CSAM network on the Darkweb. The term CSAM forum is mostly used in this dissertation; only when in a broader context referring to the larger CSAM community that extends the CSAM forum, the term CSAM network is used. The term ‘hidden service’ is used in the paper discussed in Chapter 5, as this paper is part of a series of papers written in cooperation with various law enforcement partners, in which ‘hidden services’ is the term most commonly used.

## 1.5 Aims and perspective

The main objective of this dissertation is to create insight into CSAM fora on the Darkweb, how they operate, and into the offenders who are active on them. The research questions this dissertation seeks to answer are the following:

1. How can the criminal process of Darkweb CSAM fora be characterized? (Chapter 2)
2. How organized is the crime of CSAM on the Darkweb? (Chapter 3)
3. Which offender profiles and behavioral patterns can be distinguished on Darkweb CSAM fora? (Chapter 4 and 5)
4. How can keyplayers on Darkweb CSAM fora be identified? (Chapter 6)
5. How is trust on Darkweb CSAM fora established? (Chapter 7)

A mix of qualitative as well as quantitative methods is used to answer these research questions. The current dissertation addresses these questions from multiple perspectives, including a criminological, psychological, and data science perspective.

## 1.6 Data and methods

Multiple methods are used to answer the research questions central to this dissertation. Table 1.1 provides an overview of the methods used in relation to the various research questions.

**Table 1.1 Research questions and research methods**

| Research question                                         | Research method |                               |                                                                                    |                                         |                                                              |
|-----------------------------------------------------------|-----------------|-------------------------------|------------------------------------------------------------------------------------|-----------------------------------------|--------------------------------------------------------------|
|                                                           | Literature      | Darkweb data (qualitative)    | Darkweb data (quantitative)                                                        | Police files                            | Interviews                                                   |
| 1. Criminal process (chapter 2)                           |                 | Posts and threads from 4 fora |                                                                                    | Suspect interviews from 1 investigation |                                                              |
| 2. Organization of the crime (chapter 3)                  |                 |                               |                                                                                    | Police case files from 6 investigations | Police officers and public prosecutors from 6 investigations |
| 3a. Offender profiles and behavioral patterns (chapter 4) |                 |                               | Time stamped and categorized posts from 1 forum linked to individual forum members |                                         |                                                              |
| 3b. Offender profiles and behavioral patterns (chapter 5) |                 |                               | Posts and member movements/ clicks from 1 forum                                    |                                         |                                                              |
| 4. Keyplayers (chapter 6)                                 |                 |                               | Posts and threads from 2 fora                                                      |                                         |                                                              |
| 5. Trust (chapter 7)                                      |                 |                               |                                                                                    |                                         |                                                              |

Table 1.2 provides a description of the Darkweb CSAM fora analyzed, and illustrates which fora were used for the various chapters of this dissertation.

**Table 1.2 Main characteristics of the fora**

| Forum characteristic                       | Forum A <sup>a</sup>            | Forum B   | Forum C   | Forum D   | Forum E   | Forum F   |
|--------------------------------------------|---------------------------------|-----------|-----------|-----------|-----------|-----------|
| Time span covered in the data              | 2010-2014                       | 2009-2013 | 2012-2013 | 2013      | 2014-2015 | 2015-2017 |
| Total number of forum members              | 105,650                         | 33,130    | 12,215    | 14,370    | 417,438   | 21,257    |
| Total number of posts                      | 420,000                         | 11,250    | 32,360    | 35,500    | 117,776   | 145,086   |
| Chapters in which the forum data were used | Chapter 2, Chapter 4, Chapter 6 | Chapter 2 | Chapter 2 | Chapter 2 | Chapter 5 | Chapter 6 |

<sup>a</sup> The number of forum members and posts provided here may differ from the numbers provided in the Chapters 2, 4, and 6, because within the individual studies forum members and posts may have been eliminated from the dataset based on decisions about the minimum of members' forum activity to be included in the study.

Chapters 2 and 3 pertain to qualitative analyses. In Chapter 2, a sample of posts and threads of four Darkweb CSAM fora are analyzed qualitatively in order to provide a 'crime script' (Cornish & Clarke, 2002) of the criminal process underlying these fora. Crime scripts systematically analyze the crime-commission process using a step-by-step approach, starting with the preparations necessary to access Darkweb CSAM fora and ending with the postactivity behaviors of exiting the crime scene and preventing detection. Moreover, the crime script highlights 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). In order to systematically process the data to provide input for the crime script, a qualitative thematic content analysis (Braun & Clarke, 2006) of forum posts and threads is conducted. This is a novel approach. Although the language and communication of online grooming offenders has attracted a lot of attention in recent years (e.g. Broome et al., 2020; Chiang & Grant, 2019; Kinzel, 2021; Lorenzo-Dus et al., 2020), research considering the language and communication of Darkweb CSAM offenders is still scarce.

Chapter 3 uses a more theoretical approach, and aims to answer the question how organized the crime of Darkweb CSAM is, based on existing organized crime literature. Six large-scale police case files of investigations conducted by the national as well as regional police units, and within cybercrime as well as CSAM divisions are selected. Selection took place in cooperation with specialized law enforcement personnel and cases were selected with the aim to reflect diversity. First, interviews with police officers and public prosecutors are conducted with the goal of gaining an initial insight

into Darkweb CSAM investigations and providing structure to the main analysis. In the subsequent main analysis, police case files are systematically analyzed using methods akin to the Dutch Organized Crime Monitor (Kruisbergen et al., 2018).

In the Chapters 4, 5, and 6, the Darkweb CSAM forum data are analyzed quantitatively and in various ways, in order to explore the crime of online CSAM from multiple perspectives. In Chapter 4, all posts of one of the aforementioned Darkweb CSAM fora are analyzed innovatively applying concepts, measures and methods stemming from criminal career research. To do so, posts are time stamped, categorized based on subforum topic, and linked to individual forum members by nickname. First, the evolution of the forum in terms of member numbers and the volume and nature of these members' forum activity over time is examined. Thereafter, Group-Based Trajectory Modeling (GBTM) is applied to identify distinct patterns of forum activity (in terms of the frequency and topics of posts) and the accompanying offender profiles.

For Chapter 5, the researchers not only have access to the communication data of a certain Darkweb CSAM forum, but also to all member forum movements (or clicks), regardless of them being publicly active communicators or not. This offers a unique opportunity to establish behavioral patterns of members who were not active communicators on the forum, but who did surf through and read the forum's contents (including CSAM). The term 'behavior flow' is introduced to describe the ways in which members traverse and interact with the website. More specifically, behavior flow is defined as the logged/captured clicks of a member, and the number of internal or external hyperlinks accessed by a particular member during a single session on the website. Univariate descriptions with measures of central tendency are used to describe the average time spent on the forum, the frequency of visiting, and the activities undertaken during a visit, such as subforum visits and (attempted) downloads.

Chapter 6 uses various network science methods and techniques (Barabási, 2016), including traditional social network analysis using several centrality measures, to identify keyplayers on two different Darkweb CSAM fora and to analyze the structural properties and distributions of these fora. The advantage of this approach is that anonymized datasets can be used for the analysis, and that the content of the messages posted does not have to be seen or read in order to be able to conduct the analyses. This means that researchers without clearance are also able to partake in the analysis of the data.

Finally, with Chapter 7 the empirical part of this dissertation ends with a systematic literature review from a multidisciplinary perspective (criminological as well as psychological), using six databases and a variety of search terms; resulting in a total of 21 relevant papers. The aim of this chapter is to provide an overview of the current knowledge and understanding around the nature of trust development in online net-

works, and how relationships are formed among members of these, in order to derive insights that may help explain and make better sense of the way Darkweb CSAM forum members communicate and interact with one another.

### **1.6.1 Ethical considerations**

For this PhD project, ethical approval and approval to use law enforcement data was requested from the Dutch National Prosecution Office. Approval was obtained to, within the boundaries of the current research project, use police investigation case files and Darkweb data and to interview professionals from law enforcement as well as the National Prosecution Office. Additional ethical considerations were made within the project itself.

Qualitative and quantitative research on Darkweb forum environments, using forum members' communication and other behavioral data, comes with new ethical challenges. Research involving human research subjects usually requires informed consent, yet this is impossible and undesirable to acquire in these anonymous forum environments (Markham, 2010). Previous research has considered these ethical and privacy issues when researching digital fora in general, and concludes that although informed consent cannot be obtained, the potential harm to individual forum members is minimized because they are active under a nickname, which means that their true identity remains unknown (Holt, 2010; Rutter & Smith, 2005).

Research and analysis of Darkweb CSAM 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 behaviors and experiences on these fora, it is possible that when research findings become public, forum members perceive an increased risk of apprehension, which may activate them to take extra security measures (Hutchings & Holt, 2017). This may complicate law enforcement investigations and lead to difficulties identifying offenders. One could argue that researchers should not directly or indirectly encourage this to occur. Both the present study and previous research however illustrate that subjects are already very much aware that law enforcement and other 'non like-minded' people with different intentions are present on the fora (Jenkins, 2001; Yip et al., 2013). Nevertheless, they feel anonymous enough to continue their criminal practices. Academic research on CSAM fora is therefore deemed unlikely to intervene with law enforcement's investigative efforts.

Cognizant of these ethical considerations, several precautions were taken in the present research. First of all, no direct interaction between the researchers and research subjects took place. The hidden offender population was studied in its 'natural habitat' through unobtrusive means. This comes closest to observing the offenders when they are acting the way they would without the researchers being present. Fur-

thermore, (nick)names of potential victims or offenders or other personal or identifiable information was removed from the reported post quotations (for example in Chapter 2). Moreover, given restrictions following ethical examination by the Dutch 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) were not reported.

Finally, because of the illegal character of the Darkweb CSAM fora under investigation and the CSAM available there, these fora and thus data regarding communications between forum members are off limits to most researchers (Jenkins, 2001). Access can only be acquired through designated law enforcement agencies and to law enforcement officers with special clearance. Therefore, most of the analyses that are part of this dissertation were conducted while working for such a designated law enforcement agency. Moreover, the results were interpreted in close cooperation with experts from various disciplines (operations, analysis, victim identification, data science etc.) working for the Dutch Child Exploitation Unit. This emphasizes the importance of researcher-practitioner partnerships in this particular area of research.

## **1.7 Academic and practical relevance**

### **1.7.1 Academic relevance**

As law enforcement investigations into Darkweb CSAM are challenging and time consuming, as yet, data on Darkweb CSAM crime available for academic research are still scarce. Moreover, as mentioned, Darkweb CSAM fora are not accessible to many researchers because of their illegal nature. Notwithstanding the public and research interest in CSAM on the Darkweb, this may also contribute to the relative absence of studies in this area. This lack of empirical data leads to major gaps in the existing research. For the first time, for the current dissertation large datasets of various Darkweb fora were available. Analyzing these data from multiple perspectives and using various methodologies, the current dissertation adds to the academic literature by providing new knowledge shedding light on thus far underresearched topics.

The first major gap in the extant research pertains to the offender population being researched. More specifically, most of the existing research about CSAM is based on small and limited groups of offenders. Samples in the majority of research consist of prosecuted offenders or ex-offenders now receiving treatment. Additionally, there are some self-report studies of internet users, and P2P monitoring studies. However, currently there is limited knowledge on the more hard-to-reach populations (Rimer, 2017; Westlake & Bouchard, 2016; Zulkarnine et al., 2016), such as offenders currently

active on the Darkweb. This means that the smartest and technically sophisticated offenders never caught by law enforcement have hardly been researched (Duijn & Klerks, 2014; Morselli, 2009). Only using data from known offenders can however lead to biased information. Therefore, when wanting to gain knowledge about the full population of CSAM offenders active on new online platforms, it is important to use innovative methodologies to get access to offender data that was previously off-limits to research (Aaltonen, 2021). Rather than being based on a small and limited sample of the population, the current dissertation uses large samples and, in some studies, the full population of members active on particular Darkweb CSAM fora, offering insight into a population that has not yet been caught by law enforcement nor is currently receiving treatment.

The second major gap in the extant research is that the methodologies used to explore (Darkweb) CSAM offending are currently still limited in scope. Many existing studies explore CSAM offender behavior in a traditional way, based on for example police investigation case files or suspect interviews or surveys. Studies making use of forensic digital artifacts (the memorialization of user activity left within a device or file) in order to describe and explain offender behavior are still in its infancy. However, offenders active on Darkweb CSAM fora constantly leave digital traces of their movements and offending; on the Darkweb itself as well as on the Clearnet (Sammons, 2016). The current dissertation examines these forensic digital artifacts, such as forum posts' time stamps, event logs, and forum members' registry data and digital movements, in order to describe and explain offender behavior. The advantage of this exercise is that offenders are studied in their 'natural habitat', unaware that they are being studied (though cognizant of a general risk of law enforcement surveillance). This means that the risk of socially desirable behavior is limited and that there is no dependence on secondary sources.

Making use of these forensic digital artifacts, various innovative methodologies can be implemented to explore offender behavior. Innovative methods such as those associated with the criminal career paradigm (Piquero et al., 2003) are hardly used in this particular research area (Fortin & Proulx, 2019), despite the fact that this paradigm has proven its value to examine the criminal trajectories of those engaged in sexual offending (Blokland & Lussier, 2015; Blokland, 2018). Moreover, although the importance of the social aspect of Darkweb CSAM fora is suspected, the lack of data available to academic research results in limited knowledge of the social nature and culture of CSAM fora on the Darkweb, the crime facilitating role of these fora and the organized nature of the crime commission process. In the current dissertation, however, various (network) analyses could be conducted, shedding light on the social connections and relationships of members active on Darkweb CSAM fora.

A consequence of these knowledge gaps in Darkweb CSAM related crime, is that they lead to a theoretical and conceptual backlog in cybercrime research. Existing theoretical embedding is limited to CSAM in general, and falls short when taking into account CSAM fora on the Darkweb. The internet allows for completely new forms and experiences of human sexuality and arousal, and much more research from various disciplinary angles is needed to create a full picture of the phenomenon (Carnes, 2003). If one wants to fully comprehend CSAM in the modern era, one has to approach CSAM crime also from an organized/cybercrime perspective. This would contribute to a fuller theoretical embedding of the topic.

### **1.7.2 Practical relevance**

The few studies on Darkweb CSAM that have been conducted, portray a worrying picture. As mentioned, in recent years CSAM has shown a major increase in scale, on the supply side as well as on the demand side. The numbers of offenders exchanging CSAM and their involvement seems to increase. Where in the early days, the Darkweb was limited to a few technically savvy offenders, current law enforcement and media reports counting up to hundred thousands of members on individual Darkweb fora are no exception. Not only do the numbers increase, there are also indications that the material available and exchanged on the Darkweb is becoming more extreme, including for example very young children and sadism (Europol, 2020; Woodhams et al., 2021). Furthermore, as mentioned, many offenders active on the Darkweb start their CSAM offending already at a very young age (Insoll et al., 2021). Especially for this young offender group long-term exposure to (Darkweb) CSAM may lead to normalization and positive reinforcement, and may increase illegal behavior (Yang et al., 2021). Deepened knowledge about and a better theoretical understanding of the characteristics of CSAM fora on the Darkweb, the criminal process of CSAM exchange on these fora, and of the online behaviors of individual offenders and their mutual relationships, is essential to effectively fight this crime.

In this regard, the current study offers practical guidance and knowledge that may aid law enforcement in designing their investigations. Digital investigations, especially those on the hidden and anonymous Darkweb, are complex and time-consuming, and need a great deal of (technical) expertise and experience from law enforcement (Bleakley, 2018; Raven et al., 2021). Cooperation and close partnerships between academics and law enforcement communities are valuable in this regard. Law enforcement can provide academics with the most urgent questions to be answered in order for them to do their work effectively, and academics can feed law enforcement professionals with practical translations of the most recent research findings, including recommendations for a better practice. Continuous cooperation, combined with in-

novative research, is the only way to stay up to date with the academic and practical knowledge about Darkweb CSAM offending (Insoll et al., 2021).

Finally, and most importantly, offending is inseparable from victimization. In other words, if there were no offenders, there would be no victims. Research repeatedly points out the severe impact CSAM offending has on victims. Nearly 70% of CSAM victims express the major impact of the distribution of their images, as they constantly worry about being recognized by someone who has seen images of their abuse. For many victims, the impact of knowing that the distribution of their images never ends and that they will be online forever is even more severe than the impact of the hands-on abuse they have suffered (Canadian Centre for Child Protection, 2017). Therefore, offender focused research, resulting in increased knowledge and recommendations for a better practice, ultimately also leads to a better protection of children.

## **1.8 Dissertation outline**

This dissertation commences with a study providing a detailed qualitative description of the criminal activities and processes underlying the criminal phenomenon of Darkweb CSAM fora, and the various steps involved in the exchange of CSAM on the Darkweb (Chapter 2). This is done because criminal activities are good to study in their own accord in order to later better understand the organization of offenders (Von Lampe, 2016). The second study proceeds with a qualitative and theoretical analysis of this organization and the offenders involved in it (Chapter 3). This study asks to what extent Darkweb CSAM fora can be explained from an organized crime perspective.

The research then shifts to a quantitative approach. The third study consists of an empirical analysis of the behavioral trajectories and profiles of offenders active on Darkweb CSAM fora (Chapter 4). This study describes the evolution of a large and general Darkweb CSAM forum, in terms of member numbers and the volume and nature of these members' forum activity over time. It also asks to what extent distinct forum activity patterns – in terms of the frequency and topics of posts – can be distinguished for forum members. The fourth study builds on these analyses and examines the growth of the CSAM forum member count over time, the frequency with which members are online, and it examines member behavior in more detail, such as their activity on certain subfora and their downloading activity (Chapter 5). The novelty of this study is the fact that its analyses include the behavior of forum members who have a presence on the forum, who interact with the platform by visiting the various forum environments and downloading the contents, but who are not active communicators on the forum's public environments. The fifth study takes a social network approach in

order to define and visualize forum members' relationships and to identify keyplayers and distinguish them from the regular forum members (Chapter 6). Moreover, this chapter analyses the structural properties and distributions of the fora in order to identify forum policies and processes through its underlying network.

Finally, the sixth study links individual offending motivation and behavior to the aggregation of the fora using the concept of trust (Chapter 7). This is done by means of a literature review from a criminological as well as a psychological perspective.

In closing, Chapter 8 provides a summary of the preceding study's main results and provides the dissertation's overall conclusion. Furthermore, this final chapter discusses the methodological strengths and limitations of the preceding research, describes the research finding's (policy) implications, and suggests directions for further research.



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 seized 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 collab-

oration 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 (some-

times 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 <sup>a</sup> |
| 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            |

<sup>a</sup> 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 Thompson 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 (Thompson & 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 of-

fender. 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**

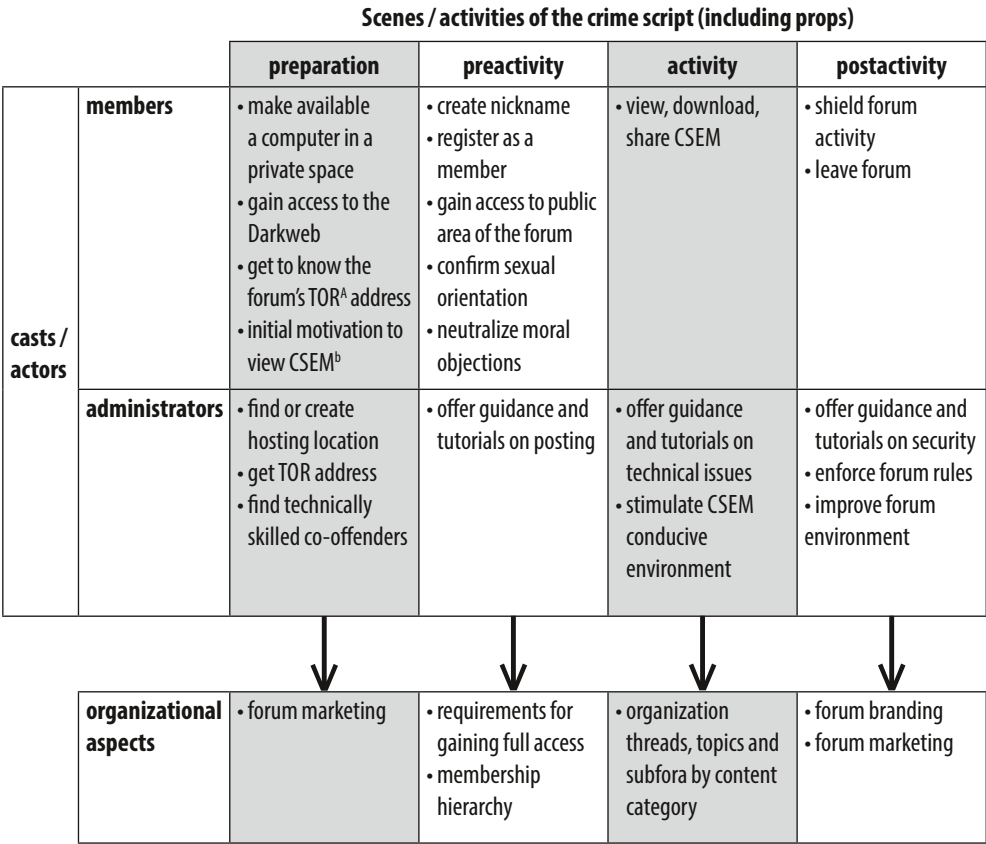
### **2.3.1 Descriptive statistics**

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**



<sup>a</sup> TOR stands for The Onion Router, an internet browser giving access to the Darkweb.  
<sup>b</sup> 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; Thompson & 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 but 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: “*gyo 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???? Pleeeeeease*.”

#### 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 ring 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 Ups.”* 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 where 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; Thompson & 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-sided 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.





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.), *Cyber-crime in Context* (pp. 259-280). Springer. [https://doi.org/10.1007/978-3-030-60527-8\\_15](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.e. 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.e. 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.<sup>1</sup> 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.

---

<sup>1</sup> 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 organ-

ize 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 advice (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

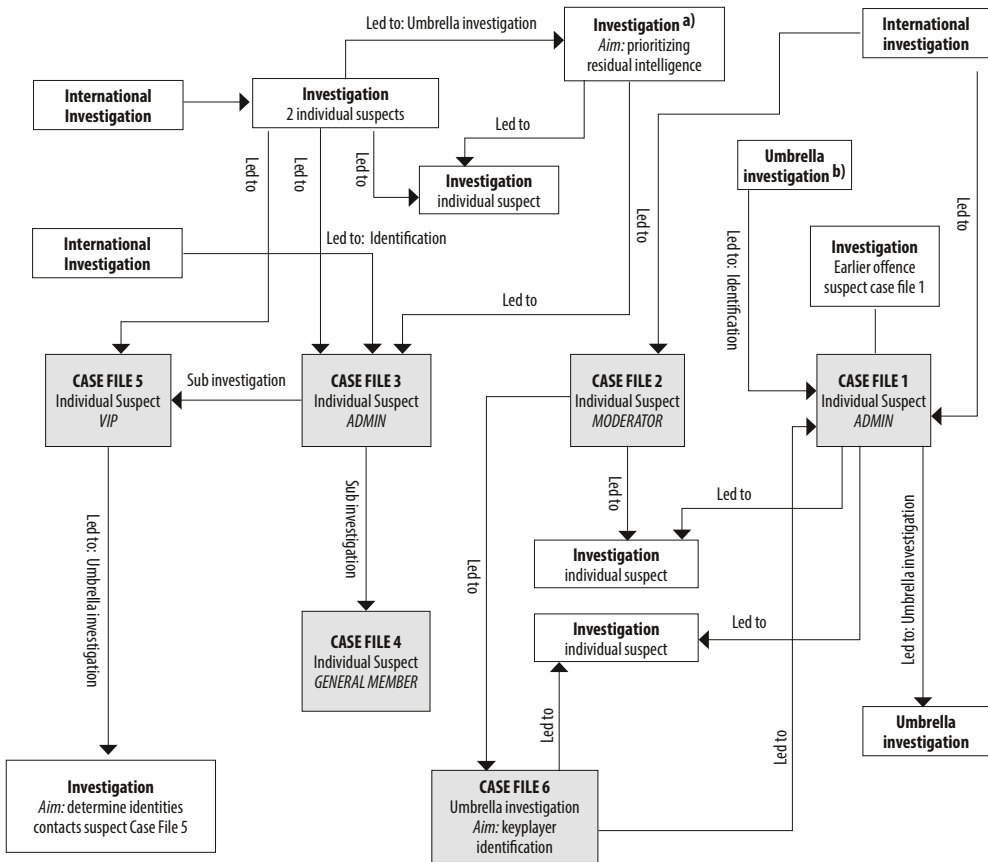
and online criminal markets, in the current study we address the organization of Darkweb CSE fora as entrepreneurial, illegal governance, as well as associational structures.

## **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**



- <sup>a</sup> 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.
- <sup>b</sup> 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 <sup>a</sup>   |
|---------------------------------------------------------------|----------------------------------------------|-------------------------------------------------------------------|-------------------------------------------------|-------------------------------------------------|-------------------------------------------------|----------------------------|
| <b>Case information</b>                                       |                                              |                                                                   |                                                 |                                                 |                                                 |                            |
| 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                    |
| <b>Suspect information</b>                                    |                                              |                                                                   |                                                 |                                                 |                                                 |                            |
| 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 <sup>b</sup>                         | 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 <sup>c</sup>                          | >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 <sup>d</sup>    | 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.                       |
| <b>Related information</b>                                    |                                              |                                                                   |                                                 |                                                 |                                                 |                            |
| Information on number of related suspects and identifications | 10-20<br>1 identification                    | 10-20                                                             | >20<br>2 identifications                        | 1                                               | -                                               | 10-20<br>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 <sup>a</sup> |
|------------------------------|--------------------|--------------------|-------------------|--------------------|-------------------|--------------------------|
| <b>Interview information</b> |                    |                    |                   |                    |                   |                          |
| Interviewed person           | Police coordinator | Police team leader | Public Prosecutor | Police team leader | Public Prosecutor | Police team leader       |

- <sup>a</sup> 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.
- <sup>b</sup> 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.
- <sup>c</sup> 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.
- <sup>d</sup> CP stands for child pornography

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

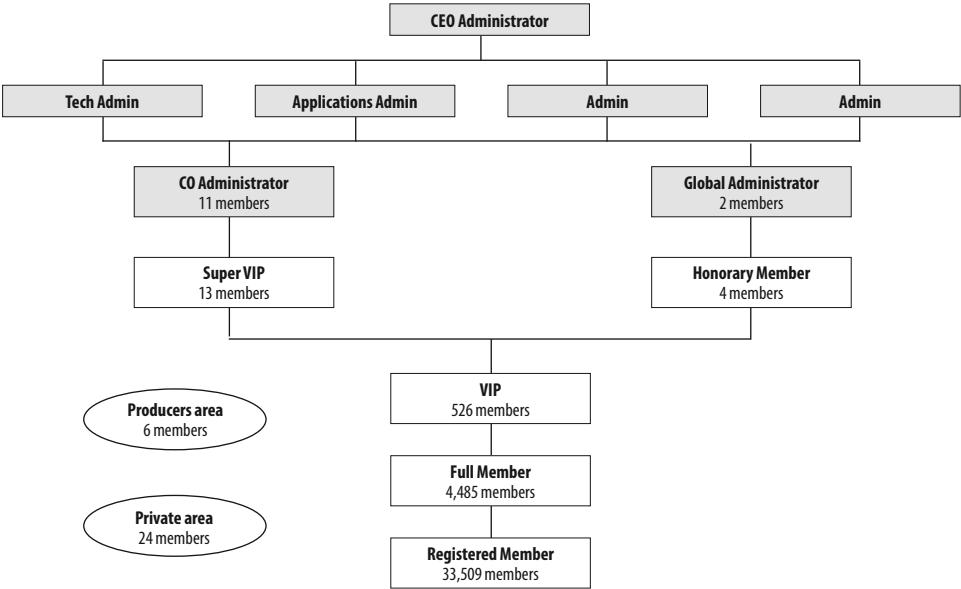
The interviewees describe Darkweb CSE fora as digital marketplaces, in which illegal goods and services are voluntarily offered and exchanged and where there is overlap between suppliers and demanders. By using the Darkweb as the platform for these fora, and by giving members the opportunity to operate 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 belief 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 grant 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 of 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 in-

visitation 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 ma-

terial. 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 association-al 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 possible 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.

A network diagram with nodes and connecting lines, overlaid on a dark gray background. Some nodes are represented by human silhouettes, while others are question marks. A large, stylized circular graphic is visible in the top right corner.

## CHAPTER 4

# PROFILING DARKWEB CSAM FORUM MEMBERS USING LONGITUDINAL POSTING HISTORY DATA

***This chapter has been published as:***

Van der Bruggen, M., & Blokland, A. (2021). Profiling Darkweb child sexual exploitation material forum members using longitudinal posting history data. *Social Science Computer Review*, 40(4), 865–891. <https://doi.org/10.1177/0894439321994894>

## Abstract

Darkweb fora dedicated to the illegal exchange of child sexual exploitation material (CSEM) continue to thrive. Profiling forum members based on their communication patterns will increase our insights in the dynamics of online CSEM and may aid law enforcement to identify those members that are most influential and pose the highest risk. The current study uses data from a large English language Darkweb CSEM forum that was active between 2010 and 2014, containing over 400,000 posts. Posts were time stamped, categorized based on subforum topic, and linked to individual forum members by nickname. Group-Based Trajectory Modeling (GBTM) was subsequently applied to derive forum member profiles based on members' posting history. Analyses show that over the course of the observation period overall activity levels – in terms of total number of posting members and the average number of posts per month per member – fluctuate substantially, and that multiple developmental pathways – in terms of monthly patterns in the frequency of posts by individual members – can be distinguished. Theoretical and practical ramifications of these findings are discussed.

## 4.1 Introduction

Despite the worldwide increase in law enforcement attention and evident public aversion to online child sexual exploitation material (CSEM), the illegal exchange of CSEM continues to thrive. An important explanation for this is the growing potential and speed of the internet. Platforms have emerged offering users high levels of anonymity, built-in countermeasures to hide illegal activity and reduce the risk of detection, 'on-demand' viewing, and unprecedented networking opportunities with like-minded others (Finklea, 2017; Steel et al., 2020). CSEM fora are now primarily located on the Darkweb, an encrypted part of the internet only accessible through specialized software such as the TOR webbrowser (DeMarco et al., 2018). Access to the Darkweb, and hence to Darkweb CSEM fora, is no longer limited to the technical savvy, but broadly utilized by offenders with varying technical dexterity (Goodman, 2015). While approximately 2% of TOR hidden services websites are CSEM related, estimates are that roughly 80% of TOR hidden service queries and traffic can be linked to CSEM (Owen & Savage, 2015). Academic research on Darkweb CSEM fora and their members is lim-

ited however, because, due to its content, merely accessing a Darkweb CSEM forum is illegal and would make researchers liable to prosecution.

Originating from researcher-practitioner collaboration, the current study utilizes a unique dataset pertaining to a large Darkweb CSEM forum to describe its evolution, and to profile forum members based on their online communications. More specifically, the current study aims to answer two related research questions:

1. How can the evolution of a large and general Darkweb CSEM forum be described, in terms of member numbers and the volume and nature of these members' forum activity over time?
2. Can distinct forum activity patterns – in terms of the frequency and topics of posts – be distinguished for forum members?

Answering these research questions provides insight into Darkweb CSEM forum members' online behavior and its development over time. Moreover, it shows which forum areas and content are most popular and which members are most prolific in their online communications.

#### **4.1.1 Internet fora as online communities**

On internet fora, members communicate by submitting posts and by reacting on postings of other forum members. Over time, this user-generated content develops into discussions, or 'threads', centered around certain topics. Internet fora vary greatly in their characteristics, such as its number of members, the breadth of its focus, and the duration of existence. Moreover, over time internet fora may evolve in aspects such as density, generalization, and posting intensity (Morzy, 2013). For example, whereas some fora continue to be characterized by a high 'on-topic' posting intensity, other fora morph into broad and general discussion platforms. Likewise, some fora begin small, and evolve into slightly bigger, yet still dense communities of concurring individuals, whereas other fora grow exponentially and attract many users who might not always be very active, but who use the forum primarily as a location to surf around and gain knowledge. Apart from their informative and practical usefulness, the social aspect of fora is often regarded as essential (Jin et al., 2010; Miller, 2016). As members often identify with the topic of the forum they engage in, these fora form the basis of what has been referred to as internet (micro)communities (Morzy, 2013; Özyer et al., 2013).

Research suggests that, in general, a small minority of forum members is responsible for the majority of forum activity. In fact, 'lurking' appears to be normal internet behavior, as on average lurkers are found to constitute 90% of all forum members

(Gong et al., 2015; Mousavi et al., 2017; Tagarelli & Interdonato, 2013). This may especially apply to fora dedicated to an illegal or otherwise unconventional topic (e.g. Dupont et al., 2016; Kleinberg et al., 2020). Nevertheless, lurkers are often found to be attached to the content of the forum and may derive their identity from it. This may lead them to take on a more active and engaged role at a later stage (Gong et al., 2015; Mousavi et al., 2017).

When it comes to Darkweb fora facilitating illegal behavior, knowledge on the development of such fora as a whole, as well as the behavioral trajectories of their individual members, is of great theoretical and practical value, and can contribute to allocating law enforcement resources to those fora and those members that pose the greatest risk.

#### **4.1.2 Darkweb CSEM offender communities**

Individuals who, in normal life, feel stigmatized for their norm divergent interests, or who wish to communicate about illegal topics are found to rely more heavily on the internet than individuals who wish to speak about more accepted and mundane topics of interest (Goodman, 2015). Given its high anonymity, this likely applies even more strongly to the Darkweb. On many Darkweb fora, illegal goods such as weapons and drugs are offered and sold, and cybercriminals, such as malicious hackers and phishers, gather to exchange their expert knowledge (Décary-Héту & Dupont, 2013; Dupont et al., 2017). First and foremost, these fora are criminal marketplaces: locations where illegal goods and services can be obtained (either in exchange for money or for other illegal goods and services in return) (Holt, 2012; Tzanetakis et al., 2016). Moreover, Darkweb fora allow for extensive communication on deviant topics, without being counterbalanced by the mainstream discourse (Holt et al., 2010). As such, in the Darkweb communities that emerge from these fora, crime and deviance can quickly become normalized (Van Hout & Bingham, 2013).

Unsurprisingly, CSEM communities have increasingly relocated to the Darkweb. As with other fora, Darkweb CSEM fora develop by the means of user-generated content and thus rely on users posting comments and content. The virtually anonymous nature of the Darkweb allows CSEM forum users to be forthcoming about their sexual interests and desires and makes them willing to share illegal material – and by doing so become active in building the forum’s content – with little risk of societal disapproval and stigma, and a likelihood of arrest and prosecution that is equally perceived negligible. Typically, CSEM fora enable users to submit series of posts, resulting in threads, that are placed within the various forum sections that in turn relate to topics of sexual interest (e.g. boys, girls), technical issues and forum management. Like other cybercriminal Darkweb fora, Darkweb CSEM fora function primarily as crimi-

nal marketplaces, where illegal goods – i.e. CSEM – are voluntarily exchanged between suppliers and demanders. Unlike other Darkweb marketplaces however, CSEM is often bartered rather than bought and sold, and commercial motives seem largely absent (Van der Bruggen & Blokland, 2021). CSEM fora also function to support an online community in which child abuse is normalized and even promoted, and in which forum members find respect, recognition and emotional bonding (Durkin & Bryant, 1999; Jenkins, 2001; O'Halloran & Quayle, 2010; Quinn & Forsyth, 2013; Steel et al., 2020; Van der Bruggen & Blokland, 2021).

As do other internet fora, individual CSEM fora may vary in focus, size, and duration of existence (Van der Bruggen & Blokland, 2021). Darkweb CSEM fora are typically structured by allocating members various roles, relating to their tasks, responsibilities and status within the forum community. This hierarchical order may include formal statuses like registered member, VIP member, moderator, or admin (Bartlett, 2014; Finklea, 2017; Goodman, 2015). The highest ranking members, the admins and moderators, are those members that are usually involved in establishing and managing the forum. Moreover, forum administrators and moderators typically organize the network's activities and advise and provide answers to questions from registered members (O'Connell, 2001). VIP members typically achieve their priority status because of their positive contribution to and engagement with the community. Finally, the bulk of members consist of the lower ranking members, who enter and exit the forum at any stage. These members may contribute to the forum by sharing and downloading CSEM, but they do not have a major role in the forum's development and maintenance. Lower ranking members may however, be motivated to rise within the forum's hierarchy in order to become respected, and to build a certain status. They can do this by portraying frequent forum and posting activity, by sharing increased amounts of (unique and new) child abuse material, by sharing stories and fantasies or by emotionally or technically supporting fellow forum members (O'Connell, 2001).

Against the background of prior research on internet fora in general (Morzy, 2013), and studies into the organization of CSEM fora in particular (O'Connell, 2001; Van der Bruggen & Blokland, 2021), the current study will first describe the evolution of the Darkweb CSEM forum that is the topic of this study. While the previous literature as yet offers little ground for deriving concrete hypotheses regarding the temporal development of such fora, describing this particular forum's evolution, in terms of member numbers and the volume and nature of these members' forum activity, is important to contextualize the posting behavior of individual members subsequently scrutinized.

### 4.1.3 Typologies of online CSEM offending

When trying to classify offenders according to typologies of online CSEM offending and hypothesize about patterns of forum behavior among the various types of individuals interested in CSEM, it is important to consider some of the psychology that drives individuals towards CSEM offending. Drawing on the more general theory of problematic internet use (Davis, 2001), Quayle and Taylor (2003) describe engagement with the internet by people with a sexual interest in children as a two-pronged, dynamic process in which individuals move through different stages of involvement. First, repeated exposure to online CSEM by itself is assumed to have a disinhibiting effect, fueling escalating patterns of CSEM consumption, both in frequency and severity. Second, the model recognizes the social aspect of online CSEM offending, which starts with the individual's realization that others are also engaging in the same behavior – thus providing grounds for justification of that behavior – and ends with them taking an active part in the online CSEM community. In this community, cognitive distortions regarding sexually engaging with minors and justifications for viewing and trading CSEM go unchallenged, perpetuating and further escalating individuals' offending behavior (Davis, 2001; Quayle & Taylor, 2003).

Although not yet as well developed and empirically researched as behavioral and etiological typologies of child sexual abuse offenders in general (DeMarco et al., 2018), various authors have aimed to further classify online CSEM offenders. These typologies may focus on offenders who use online communications to meet and groom minors online (DeHart et al., 2017; Tener et al., 2015; Webster et al., 2012), offender motivations for online CSEM offending (Elliott & Beech, 2009), offender behaviors related to online CSEM offending (Krone, 2004), or on a combination of the latter (Lanning, 2001). Lanning's (2001) typology of sex offenders using computers to access CSEM and sexually exploit children with its specific focus on both offender behavior and -motivation is arguably the most thorough and the most applicable to the purpose of the current study.

Lanning (2001) suggests a motivational continuum ranging from a nonsexual- to a deviant sexual motivation to underly online CSEM offending. Situational offenders, who are at one end of this continuum and search for child abuse material out of curiosity or impulsivity and who behave more opportunistic, are distinguished from preferential sex offenders, who search for child abuse material deliberately and repeatedly out of a certain sexual preference. According to Lanning (2001), both situational and preferential offenders consist of three subtypes. Among the situational offenders, 'Normal adolescents/adults' are characterized by impulsivity and curiosity, searching for online pornography and accessing wide ranges of (legal and illegal) sexual material. This subtype parallels Krone's (2004) 'Browser' type, who accidentally hits on

CSEM websites or material by browsing or responding to spam, and then knowingly saves the content. Second, ‘Morally indiscriminate offenders’ are sex offenders with a history of varied violent offenses and are primarily power/anger motivated. Finally, ‘Profiteers’ consider the crime of online CSEM with its low risk of identification as a lucrative way of making profit. Elliott and Beech (2009) alternatively label this group ‘Commercial exploitation offenders’.

Among preferential offenders, Lanning (2001) firstly distinguishes ‘Pedophiles’, who have a definite sexual preference for children. A second group of preferential offenders, ‘Diverse offenders’, has various deviant sexual interests, not specifically aimed at children. Finally, ‘Latent offenders’ potentially have illegal sexual preferences, but only start to act out when inhibitions are weakened and preferences are validated through online engagement and communication, mirroring the social part of the Quayle and Taylor (2003) model. These different types of preferential offenders parallel the ‘Secure collector’ subtype within Krone’s (2004) typology, who tends to be security minded and actively seeks material through secure networks.

The three-left hand columns of Table 4.1 summarize and describe the subtypes within Lanning’s (2001) typology.

**Table 4.1 Typology of online CSEM offenders (Lanning, 2001) and their hypothesized forum behavior**

| Motivation  | Type                            | Explanation                                                                                                                        | Hypothesized first forum activity                           | Hypothesized posting frequency | Hypothesized posting duration | Hypothesized posting focus                                                       |
|-------------|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------|--------------------------------|-------------------------------|----------------------------------------------------------------------------------|
| Situational | ‘Normal’ adolescent/adult       | Searching for online pornography out of impulsiveness/curiosity, leading to access to illegal pornography and sexual opportunities | Later stage (when the forum is most popular and accessible) | Relatively infrequent          | Relatively short              | When communicating at all: superficial and short, no focus on community building |
|             | Morally indiscriminate offender | Power-anger motivated, potential history of violent offenses                                                                       | Could both be at an early or later stage                    | Intermediate                   | Intermediate                  | Mainly on sexual topics, no focus on community building                          |
|             | Profiteer                       | Financially motivated                                                                                                              | n/a                                                         | n/a                            | n/a                           | n/a                                                                              |

| Motivation   | Type             | Explanation                                                                                     | Hypothesized first forum activity                      | Hypothesized posting frequency | Hypothesized posting duration | Hypothesized posting focus                                      |
|--------------|------------------|-------------------------------------------------------------------------------------------------|--------------------------------------------------------|--------------------------------|-------------------------------|-----------------------------------------------------------------|
| Preferential | Pedophile        | Definite preference for children                                                                | Early stage (before the bulk of members become active) | Frequent                       | Longer                        | Community building                                              |
|              | Diverse offender | Wide variety of paraphilic/deviant sexual interests, no specific sexual preference for children | Could both be at an early or later stage               | Intermediate                   | Intermediate                  | On a variation of sexual topics, no focus on community building |
|              | Latent offender  | Illegal and previously latent sexual preferences are validated online                           | Later stage                                            | Increasing posting behavior    | Longer                        | Increasing focus on community building                          |

#### 4.1.4 Different dimensions of forum members' online activity

In analyzing CSEM forum members' online behavior, we build on the criminal career paradigm (Piquero et al., 2003), an analytic approach that breaks down the longitudinal sequence of individual criminal behavior into several distinct dimensions, like onset, frequency, duration and crime mix (Blumstein et al., 1988). Whereas the criminal career paradigm is increasingly being used to examine the criminal trajectories of those who engage in sexual offending (Blokland & Lussier, 2015; Blokland, 2018), up to this date this approach is only sparsely applied to online CSEM offending (Fortin & Proulx, 2019; Westlake & Bouchard, 2015). Westlake and Bouchard (2015) applied the criminal career paradigm at the macro level to identify CSEM websites with the highest survival rate. At a micro level, Fortin and Proulx (2019) examined the content of hard disks belonging to males arrested and convicted for collecting CSEM online, and distinguished four developmental patterns based on monthly changes in the nature of the depicted abuse and the age of the child victims: a degenerating spiral pattern (37.5% of the sampled collections) – collections showing an increase in the severity of the depicted abuse and a decrease in the children's age -, the sexualized adolescent pattern (20%) – showing an increase in both the severity of the abuse and the victim's age -, a boy/girl-love pattern (20%) – showing a decrease in severity and victim's age -, and a de-escalation pattern (22.5%) – showing a decrease in severity and children

of increasing age. These patterns are taken to reflect offenders' sexual interests and habituation, but could also reflect the availability (or rather the lack thereof) of certain types of content.

Similarly using a micro-level criminal career approach, individuals' Darkweb cSEM forum behavior can be broken down into several dimensions. These dimensions include onset – or the timing of the first post, frequency – the number of posts during a certain time period, duration – the time between the first and the last known posting, and nature or mix – the topics of these posts. Applying these dimensions to Darkweb forum members' posting behavior allows for a fine grained description of different online behavioral patterns and the divergence or convergence of these patterns over time. Distinguishing different dimensions in individuals' posting behavior also allows for formulating more detailed hypotheses about the online behavioral patterns of Lanning's (2001) subtypes of online cSEM offenders.

#### 4.1.5 Hypotheses

1. *The posting careers of situationally motivated normal adolescents/adults will show a late onset, low frequency, and short duration.*

According to Lanning (2001), situationally motivated normal adolescents/adults are not determinedly looking for Darkweb cSEM fora. It can therefore be assumed that they are not part of the 'in-crowd' of the cSEM community, and will only become active on the forum at a later stage of its development, when the forum becomes more well-known to the broader group of Darkweb users. Because this type of offender is primarily driven by curiosity, and not by an entrenched or looming sexual interest in minors, it is expected that their posting will be infrequent and only span a short period of time.

2. *The posting careers of morally indiscriminate offenders will show an intermediate onset, frequency, and duration, and will be predominantly sexual rather than social in nature.*

Depending on the level of previous engagement with (Darkweb) cSEM communities, the morally indiscriminate offender could first become active at earlier as well as later stages of the forum's existence. Because of them being power/anger motivated, we expect their posts to be sexual rather than social and community-focused in nature. Moreover, because of their violent inclination, morally indiscriminate offenders may also show a preference for hardcore, rather than softcore material. Hardcore cSEM is typically violent and sexually diverse nature, rather than focused on 'the love for children'.

Given that previous qualitative studies of the forum analyzed here give no reason to presume that on this particular forum CSEM is exchanged for commercial purposes (Van der Bruggen & Blokland, 2021), Lanning's (2001) profiteer type offender is therefore rendered not applicable to the forum under scrutiny.

3. *The posting careers of preferentially motivated pedophiles will show an early onset, high frequency and long duration, and will be both sexual and social in nature.*

Preferentially motivated pedophiles are hypothesized to be most dedicated to the Darkweb CSEM community. Hence, they are the group most likely to have a role in the forum's organization and be active in its earliest stages. Moreover, they are likely to portray frequent posting behavior for longer periods of time, and, besides having a sexual interest in minors, show a serious interest in and dedication to the social aspect of the CSEM community. Finally, they are likely to specifically search for material that matches their sexual preference.

4. *The posting careers of diverse offenders will show an intermediate onset, frequency and duration, and will be predominantly sexual rather than social in nature.*

Due to their wide variety of deviant sexual interest, diverse offenders are hypothesized to be dedicated to the specific CSEM forum and to the Darkweb CSEM community as a whole to a lesser degree than the pedophile subgroup. While their diverse sexual interests may translate into frequent posting behavior over extended periods of time, it will not be as focused on community building than that of the pedophile subgroup. Similar to the morally indiscriminate offender, the diverse offender is likely to collect and share material of any sexual content.

5. *The posting careers of latent offenders will show a late onset, increasing frequency and long duration, and will for a large part be social in nature.*

Finally, the latent offender is expected to portray a late onset, escalating offending pattern. New to the CSEM community, this offender group is likely to first become active at a later stage of the forum's development. Encouraged and validated by the forum environment, over time their latent sexual preferences become more entrenched, and their posting behavior is expected to increase accordingly. Latent offenders can become active CSEM community members, and over time the nature of their posts is therefore expected to reflect both the sexual and social aspects of their online behavior.

The right section of Table 4.1 summarizes hypotheses relating to how the various online CSEM offender subtypes translate to the different dimensions of their forum behavior.

## 4.2 Methods

### 4.2.1 Data collection

To describe the evolution of a Darkweb CSEM forum and explore possible patterns in forum members' posting behavior, data from an English language Darkweb CSEM forum were collected. The forum was selected after consulting experts from a dedicated law enforcement child exploitation team and based on its general nature and large size. Forum information originated from international law enforcement investigations and was available within the premises of the federal police unit. Data collection took place in conjunction with a senior software engineer working for the Dutch law enforcement's cybercrime division, using a proprietary tool for forensic data analysis. This tool was a police in-house developed software tool to automatically prepare, congregate, structure, and process large amounts of digital data in order to enable further analysis. The comprehensiveness of the data was checked by creating overviews and visualizations of all forum threads, topics, and titles.

### 4.2.2 Forum posts and categorization

The above process resulted in a dataset of all posts submitted to the selected forum for the complete period that the forum was known to be online, which was December 2010 to December 2014, when the forum was taken down by law enforcement agencies. The posts submitted to the forum were time stamped and linked to individual forum members by their online nickname. Next, a person-month dataset was constructed that for each forum member for each month of the observation period, counted the number of posts under a certain topic category. The number and topics of posts were then used to analyze both the development of the forum as a whole, as well as the behavioral development of its individual members. Table 4.2 summarizes the characteristics of the forum.

**Table 4.2 Characteristics of the forum**

| Forum characteristic              | Forum characteristic outcome  |
|-----------------------------------|-------------------------------|
| Available data                    | December 2010 – December 2014 |
| Observation period                | 49 months                     |
| # Threads                         | 105,616                       |
| # Subfora                         | 34                            |
| # Unique posts                    | 420,222                       |
| # Unique posting members          | 14,838                        |
| Average # posts per month         | 8,576                         |
| Average # posts per active member | 28.3                          |

Using forum posts as the unit of analysis introduces some important caveats best mentioned upfront. First of all, the dataset contained posts from the publicly accessible part of the forum. There was no access to messages that were exchanged between individual members privately. As it may be expected that forum members share the most personal and sensitive information privately, not having access to these communications is a first limitation of the current study. Moreover, given the nature of the available data, we are only able to analyze the evolution of the forum and the behavioral patterns of its members based on the posting behavior of those forum members who are communicatively active on the forum. Hence, we do not have information on the number or online behavior of those only 'lurking' on the forum, but not participating in its online communications. Given prior estimates, the total number of unique visitors to the forum during the observation period is expected to be much larger than the total number of posting members (Gong et al., 2015; Mousavi et al., 2017; Tagarelli & Interdonato, 2013). However, the forum under scrutiny had an application process where new forum members had to make a formal application post before gaining access to the contents of the website. This post had to contain a certain amount of CSEM, meant for new forum members to show their willingness to participate in the community and for them to prove that they were not law enforcement. Furthermore, the forum enforced a policy requiring members to contribute to the forum at least once a month for them to maintain full access to the forum. Because of these procedures, it is expected that the share of lurkers is lower for this particular forum compared to other internet fora.

Forum posts were first categorized based on the thread they originated from. As the forum consisted of large numbers of threads ( $N=105.616$ ), further categorization took place on the subforum level. The subforum is assigned by the forum itself, and consists of a forum webpage where content of a certain topic (for example hardcore, softcore, boys, girls) is gathered. As the current forum listed 34 subfora, a final manual categorization was conducted. This categorization was done based on the content of the thread- and subforum title. For example, a thread title such as 'Safe surfing on Tor using PGP' or a subforum title such as 'Tech Zone' was categorized under the category 'Information and technical safety'. When a thread title was applicable to more than one category, the subforum title was leading for deciding to which category the posts was assigned. For example, a thread title such as 'My first anal, 3y old boy' originating from a subforum called 'Hardcore' was categorized under the category 'Boys hardcore'. This final categorization yielded eight mutually exclusive categories: CSEM general, Girls Softcore, Girls Hardcore, Boys Softcore, Boys Hardcore, General discussion, Information and technical safety, and Restricted areas.

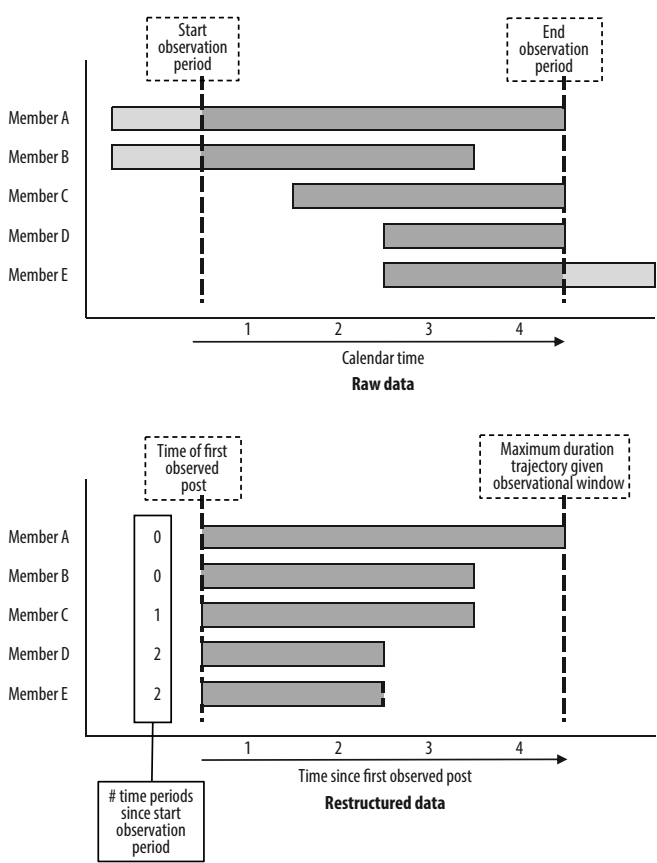
### 4.2.3 Forum member roles

Forum posts were linked to the nickname individual members were obliged to choose when registering as a member. On the forum under scrutiny, forum administrators assigned forum members with one of a number of statuses. Each status came with different privileges and levels of access to the forum. For the purpose of our analyses, we distinguish ‘Administrators’, the highest ranking category that included the Head administrator, Administrators and Co-administrators, and Global moderators; ‘VIPs’, privileged members including Producers, svip, vip, and other honorary members; ‘Registered members’; ‘Full members’; and ‘Inactive members’. The latter three categories were differentiated by the extent to which they were able to meet the forum’s posting requirements. Registered members are in the process of getting full access to the forum and are awaiting approval of their mandatory application post by the forum administrator. Once the content of this initial post is evaluated and their application is approved, the registered member is upgraded to ‘Full member’ and granted full access to the forum (excluding restricted areas only accessible for VIPs and Administrators). In the event full members subsequently were not able to meet the required level of monthly activity on the forum, they could be downgraded to ‘Inactive members’ and consequently lose full access to the forum.

### 4.2.4 Analytic strategy

The current study applied the method of Group-Based Trajectory Modeling (GBTM) using the Traj plug-in for Stata 13 (Jones & Nagin, 2013; Nagin, 2005). GBTM applies finite mixture modelling to cluster longitudinal data in a discrete number of trajectories that are allowed to vary both in level and in shape. Since their introduction in the mid-1990s, GBTMs have been used by criminologists and developmental psychologists to distinguish developmental patterns in various outcome behaviors including violence, delinquency and crime. Though different in topic and scope, what most of these studies have in common is that models are estimated on data covering some fixed time period that is demarcated by respondents’ calendar age. Hence, any developments observed in the trajectories distinguished can directly be linked to different time periods in the individual’s life span. In turn, this has fueled offender categorizations like ‘adolescence-limited’ or ‘adult-onset’. In the present study however, we have no information on forum members’ calendar age. Instead, for each posting forum member, the start of the posting trajectory is defined by the moment of the first post. Any developments in a member’s posting behavior are therefore to be interpreted against the number of months that that particular member is active on the forum under study. Figure 4.1 illustrates the implications of restructuring the data in this way.

**Figure 4.1 Schematic representation of the effects of restructuring the longitudinal posting data for five hypothetical forum members**



One important caveat of defining developmental trajectories this way is that for an unknown portion of members, the posting trajectory may be left-censored – i.e. these members may have posted their first post on the forum already prior to the start of the current study’s observational window (members A and B in Figure 4.1). Their first post observed may therefore not signal their actual introduction to the forum. While we have no way of knowing how long members may have been active on the forum prior to their first observed post, we can relate the timing of that first post to the start of the observational window. The longer the time period between the start of the study’s observation period and a particular member’s first post, the more confident we can be that this post represents the first activity of that member on the forum under scrutiny. Given the overall development of the forum under scrutiny however (see the Results section), left censoring does not seem very problematic for our analysis.

Data may also be right-censored (member E in Figure 4.1), when individual behavior continues after observation and data collection have stopped. In the present case however, the observation period ends with law enforcement taking down the forum, hence all members still active were forced to stop their posting on the forum. While for all posting forum members the end of their observed trajectory is therefore demarcated by the end of the observational window, the period between members' first observed post and the end of the observational window varies. When grouping forum members based on the patterning of their posting behavior, this may result in groups for whom the number of observations – that is, time periods over which data is available – varies.

GBTM probabilistically assigns members to each of the trajectory groups. For the current analysis members were assigned to the group with the highest posterior probability of assignment. This allowed for a formal comparison of posting behavior across trajectory groups using one-way ANOVA. As analysis evidenced unequal variances (variance ratio exceeding 1.5), and trajectory groups of unequal size, we employed the Brown-Forsythe and Welch ANOVA versions followed by Games-Howell post hoc tests. These analyses were conducted using SPSS 24.

## 4.3 Results

### 4.3.1 Descriptive analysis

Table 4.3 provides descriptives for the forum under scrutiny. In total, the forum consisted of 420,222 posts, posted by 14,838 unique members. The topic 'cSEM general' has the largest number of posts and the largest number of posting members. This is because this subforum included the 'Applications' subforum where all prospective members were obliged to post a first message in order to receive membership status. The topic 'Girls hardcore' is the second most popular topic both in terms of number of posts ( $N=89,493$ ) as in the number of posting members ( $N=4,874$ ). Both 'boy' categories are less popular, which might reflect a tendency for those with a sexual preference for boys to visit dedicated boy fora. Both hardcore categories (girls and boys) are more popular than soft core categories.

As expected, administrators make up only a very small proportion of the total number of individuals active on the forum, but are responsible for a disproportionately large part of the communications. The same applies – be it to a far lesser extent – to members with VIP status.

**Table 4.3 Descriptives of the Darkweb CSEM forum, December 2010 to December 2014**

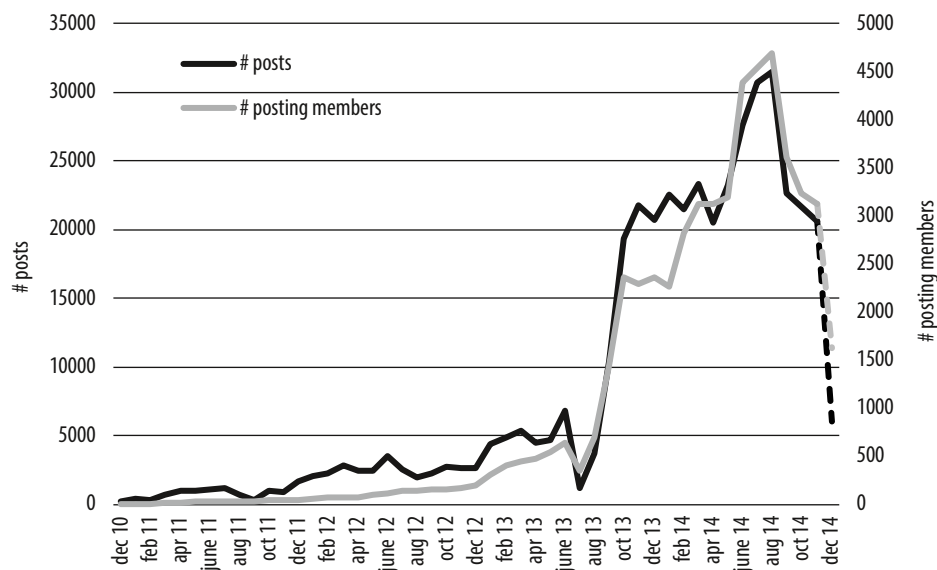
|                                         | # posts | % posts | # members | % members | # posts per member | this category includes                                                                                                    |
|-----------------------------------------|---------|---------|-----------|-----------|--------------------|---------------------------------------------------------------------------------------------------------------------------|
| <b>Total</b>                            | 420,222 | 100.0   | 14,838    | 100.0     | 28.3               |                                                                                                                           |
| <b>CSEM general</b>                     | 161,104 | 38.3    | 142,08    | 95.8      | 11.3               | Applications, Webcams, Request Zone, Studios, Amateur                                                                     |
| <b>Girls hardcore</b>                   | 89,493  | 21.3    | 4,874     | 32.8      | 18.4               | Girls hard                                                                                                                |
| <b>General discussion</b>               | 47,304  | 11.3    | 2,338     | 15.8      | 20.2               | General, Misc, Stories, Discussion Board                                                                                  |
| <b>Boys hardcore</b>                    | 36,497  | 8.7     | 2,280     | 15.4      | 16.0               | Boys hard                                                                                                                 |
| <b>Girls softcore</b>                   | 28,964  | 6.9     | 2,751     | 18.5      | 10.5               | Girls non-nude, Girls Jailbait, Girls soft                                                                                |
| <b>Restricted areas</b>                 | 25,207  | 6.0     | 891       | 6.0       | 28.3               | VIP, Producer Lounge, Private Zone, SVIP, VIP zone, Boys VIP, Girls VIP                                                   |
| <b>Boy softcore</b>                     | 20,488  | 4.9     | 1,351     | 9.1       | 15.2               | Boys non-nude, Boys Jailbait, Boys soft                                                                                   |
| <b>Information and technical safety</b> | 11,165  | 2.7     | 1,395     | 9.4       | 8.0                | Rules and Tutorials, Tech Zone, Safety, Team Zone, When the chips are down, Forum world, Welcome, Tutorials, Translations |
| <b>Administrators</b>                   | 64,743  | 15.4    | 22        | 0.1       | 2942.9             | Head Administrator, Administrator, Co-Admins, Global moderator, Producers                                                 |
| <b>VIPs</b>                             | 133,167 | 31.7    | 544       | 3.7       | 244.8              | SVIP, Honorary member, VIP                                                                                                |
| <b>Full member</b>                      | 141,954 | 33.8    | 4,480     | 30.2      | 31.7               | Full member                                                                                                               |
| <b>Registered member</b>                | 10,584  | 2.5     | 5,132     | 34.6      | 2.1                | Registered member                                                                                                         |
| <b>Inactive member</b>                  | 50,262  | 12.0    | 4,565     | 30.8      | 11.0               | Inactive member                                                                                                           |

Note The number of posting members per topic does not add up to the total number of members as members may post under multiple topics.  
The number of members per formal status adds up to the total number of members as members are allocated only one formal status.

### 4.3.2 Forum evolution

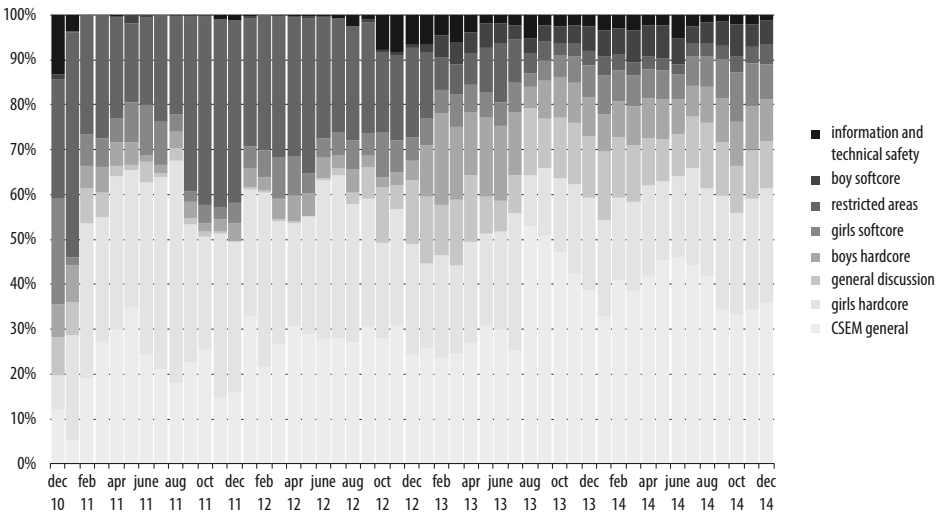
To answer our first research question, we add a temporal dimension to our descriptive analyses and describe the evolution of the forum, in terms of member numbers and the volume and nature of its communications. Figure 4.2 depicts both the total number of posts as well as the total number of unique members posting on the forum for each month of the observation period. Figure 4.2 shows the forum's evolution can be broken down in a 'start-up' period and a 'fully functional' period. During the first 32 months (December 2010 – July 2013) the number of posts is relatively low and increases to a maximum of 2,353 per month. The number of active members is also low, topping at a maximum of 638 during this period. As of September 2013 however, the number of posts increases steeply, from 10,415 post in September 2013 to a peak of 31,412 posts in August 2014. As is evident from Figure 4.2, this rise in forum activity is due to a simultaneous steep rise in the number of posting members which increases from 1,442 in September 2013 to a peak of 4,691 in August 2014. Put another way, between September 2013 and August 2014 over 700 new members enter the forum each month. The average number of posts per posting member decreases during this period, suggesting that the forum is attracting an increasingly broad array of individuals. This interpretation of forum evolution is supported by additional analysis showing that the share of administrators among posting members steadily decreases from one third early 2011 to less than 1% as of October 2013 – this despite the absolute number of posting administrators increasing from 3 during the first 3 months of observations to around 20 in the spring of 2014. With the number of forum members increasing, it is only logical that more administrators are needed to manage the forum. Subsequent analysis of the underlying case file showed that in August 2013 the forum went temporarily offline only to return with a new head administrator and new hosting platform. Under this new administrator the forum became an open forum (open to new registrations) and various new topic areas were added. The restricted areas remained available for members with a certain status, but the bulk of new forum members did not have access to these VIP areas.

**Figure 4.2 Number of posts and number of unique posting members per month**



The monthly percentual distribution of posts per topic is given in Figure 4.3. Posts in the ‘CSEM general’ category are prevalent across the entire observation period. In part, this can be explained by the continuous influx of new members posting their mandatory entrance application under this topic. Moreover, this category includes the ‘Request Zone’, which is where members can request certain material from other members. In terms of victim gender, the forum becomes slightly more balanced over time, the number of ‘girls hardcore’ posts giving way to posts under the ‘boys hardcore’ category, possibly reflecting growing variation in members’ sexual interests. The monthly distribution of posts across topic also illustrates the finding that during the first half of the observation period forum access is restricted to a small group of ‘in-crowd’ members, with much of the communication going on in the ‘restricted areas’ part of the forum. During the second half of the observation window, the number of posts in the ‘general discussion’ category increases, reflecting the growing social function of the forum. Educating new members on how to safely upload and exchange CSEM material also becomes more important, as is evidenced by the increase in posts under the ‘information and technical safety’ category.

**Figure 4.3 Percentual distribution of the total number of monthly posts across topic category**



**4.3.3 Forum members’ communication patterns**

In line with prior research on internet fora, we find that the distribution of posts is heavily skewed, with a minority of members being responsible for the lion share of all communication on the CSEM forum (Figure 4.4). 36% of forum members only contribute a single post to the forum, their posts representing 1.3% of all posts. Again, this likely reflects the forum’s policy to demand from potential members to make at least one obligatory post to the forum before gaining access to CSEM. If given the opportunity, forum members with a low number of posts might have chosen only to ‘lurk’. The 109 most active members (0.7% of all members), each contributing over 500 posts, on the other hand account for 40% of the forum’s public communications. Analyses in which we broke down the number of posts and posting members by topic reveal a similar skew in posting across topics.

Next, we examined the diversity of individual members’ posting behavior. Diversity was calculated using an adjusted version of the Simpson diversity index that ranges from 0, indicating that all posts are under a single topic, to 1, indicating an equal spread of posts across topics (Simpson, 1949). We calculated diversity for each forum member that posted at least two separate posts (64% of the total sample). Figure 4.5 shows the diversity of the totality of an individual member’s posting behavior by the total number of posts for that member. The size of the circles is relative to the number of members showing a certain total amount of posts and a given diversity. Figure 4.5 shows that diversity is higher among more active members. In fact, of those members posting between over a 100 posts, only 5.2% has a diversity below 0.5.

**Figure 4.4 Distribution of posts (December 2010 to December 2014)**

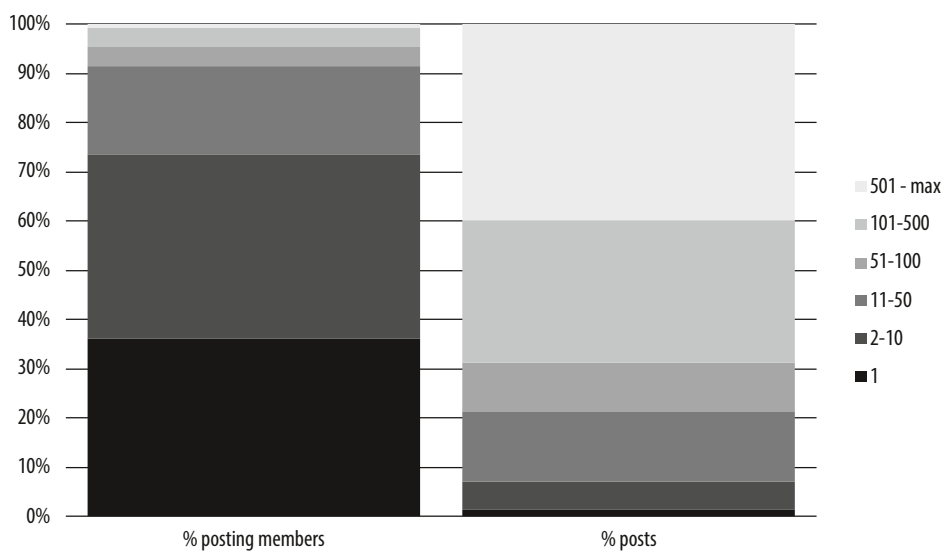
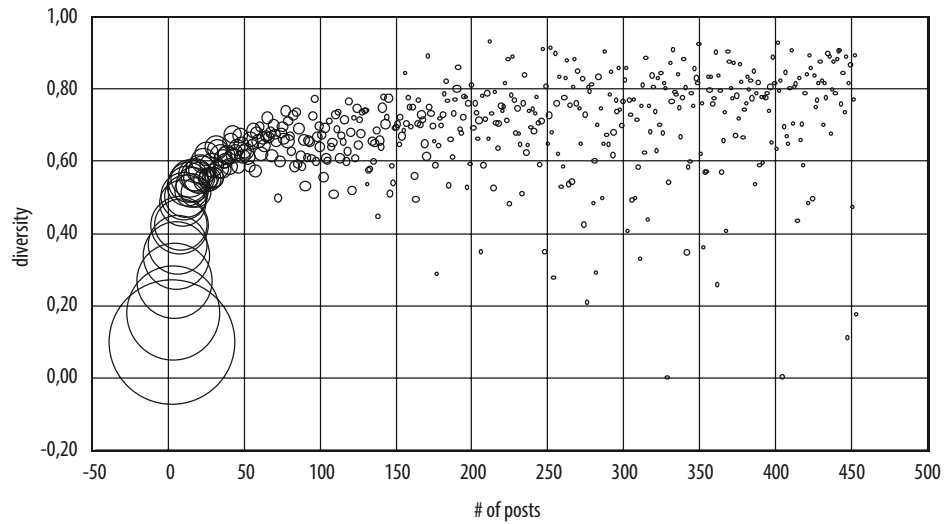


**Figure 4.5 Diversity of the total posting volume by total number of posts**



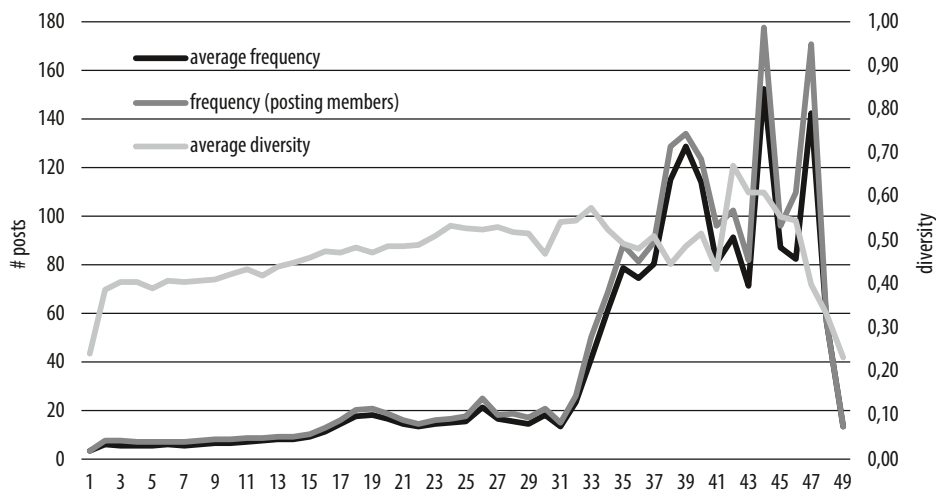
By structuring the data based on the month of first post (right-hand side of Figure 4.1), we can shift our attention from the evolution of the forum as a whole (i.e. calendar time on the x-axis) to the development of individual members' posting behavior as their posting 'career' on the forum progresses (i.e. month since first post on the x-axis). Figure 4.6 shows the average number of posts per member and the average num-

ber of posts per posting member for each month of members' posting career, as well as the average diversity of the posts across different topics. Unlike in Figure 4.5, where diversity was calculated across members' entire posting career, in this analysis, diversity was calculated on a monthly basis, only including months with at least two posts.

From the line depicting the average number of posts it can be concluded that posting frequency increases the longer members remain active on the forum. Figure 4.6 further shows that posting diversity is positively related to the length of the posting career: the average monthly diversity of posts shows an increasing trend across the number of months since the first post.

Figure 4.6 does show a sharp increase in the number of posts for those members whose posting career exceeds 31 months. Importantly, this increase is not simply the same as that shown in Figure 4.2, though both developments are related. Rather, the increase in Figure 4.6 results from selection. Like overall posting frequency, the distribution of posting career duration – that is, the number of months between a member's first and last post – is heavily skewed. The average posting career lasts for only 3.25 months, and the posts of 54.7% of members are concentrated within a single month. Therefore, with increasing length of the posting career, increasingly fewer members contribute to the average posting frequency depicted in Figure 4.6. Given the total length of the observation period (49 months), for every consequent month the averages in Figure 4.6 increasingly reflect the posting behavior of members who were already active during the 'start up' period of the forum and whose careers appear characterized by a high posting frequency. As such, Figure 4.6 underscores the need to distinguish between different CSEM forum member types based on their posting histories.

**Figure 4.6 The average number of posts and the average diversity of posting by members' posting career duration**



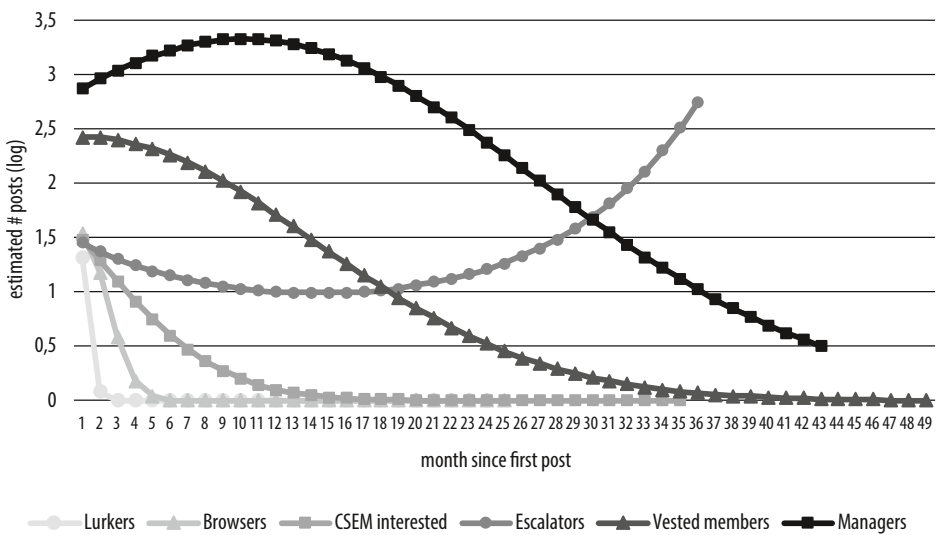
#### 4.3.4 Distinguishing member types based on their posting trajectory

We used GBTM to distinguish distinct posting trajectories. Estimating the group based trajectory models, two issues became apparent. First, given both the large number of forum members and the large number of observations per member, estimating trajectory models on the total sample would take untenably long. Hence, to keep analysis time within limits, we drew a random 10% analysis sample ( $N=1,502$ ) of all forum members to perform the GBTM. Standardized differences comparing this 10% sample to the remaining 90% of the original sample on relevant characteristics, like the average number of posts and the number of members actively posting (overall and across different topics), the average month of first and last post, and distribution of formal member statuses, revealed no significant differences between these subsamples (see Appendix Table A1). Therefore, we are confident that our analysis sample adequately reflects the forum's membership as a whole. Second, to deal with the large differences in the number of monthly posts per member, we log transformed the raw post counts, effectively reducing the skew in the data.

We estimated GBTM with up to seven groups. Model fit was assessed by the Bayesian information criteria (BIC), Akaike information criteria (AIC), and LL values, as well as additional criteria of model fit mentioned by Nagin (2005). Information with regard to model fit is provided in Table A2 in the Appendix. We found that BIC and AIC values continued to increase with each new group added – a feature commonly observed in large samples

with many observations. The six group model however, was the first to identify an upward trajectory. While the seven group model outperformed the six group model on statistical grounds, substantively the seven group model added little besides further subdividing the trajectory group showing a steep downward slope based on the number of posts in the initial months of members' posting careers. For reasons of parsimony, we therefore chose the six group model to summarize our data. We also found that models using quadratic terms to capture developments in members' posting behavior outperformed models using cubic terms. Hence, we present the trajectories from the six group, second order model. To test the robustness of these findings, we re-ran the GBTM analyses on another nine random 10% samples. These analyses showed that for these additional samples, the increase in model fit when adding trajectory groups showed a pattern highly similar to that of the original 10% sample, as did the shape and level of the trajectories distinguished.<sup>1</sup> Hence, we conclude our findings to be robust in this respect.

**Figure 4.7 Trajectories based on the frequency of total monthly posts per month since first post**



<sup>1</sup> The results for the analysis on the additional 10% samples are highly similar to those found on the first 10% sample, with two exceptions. First, in a number of samples the four or five group solution failed to converge. As the six and seven group solution always did, and BIC values indicated that the six group model is preferred over simpler models, this does not affect our conclusions. Second, while in all samples a high frequency group is detected, the shape of this trajectory depends on the maximum number of months individuals allocated to this group have been observed. In a number of subsamples, the 'managers' trajectory is based on individuals who were observed for only 25-30 months of the maximum 49 month follow up, and consequently does not show a decline in the frequency of posts during the second half of the maximum observation period.

Figure 4.7 depicts the six trajectories distinguished in our data. Again, like in Figure 4.6, the x-axis represents the number of months since the first post on the forum. Note that the y-axis depicts the estimated number of monthly posts on a logarithmic scale. Table 4.4 provides descriptives for the posting careers of each of the distinguished trajectory groups.

The largest group of forum members ( $N=883$ , 58.8% of the sample) shows very little forum activity. With an average of 2.07 total posts per member of which on average 1.61 post in the 'General cSEM' category, for many in this trajectory their obligatory introduction post seems the only registered activity on the forum. Members allocated to this trajectory enter the forum during its later stages (average month of first post is March 2014), and mostly refrain from posting shortly after that (average posting duration of 0.10 months). Given that this still leaves 9 months of observation, the short duration of these members' posting career does not seem an artefact of the forum being taken offline. Given their failure to regularly contribute to the forum's content, these members would have quickly lost access to most of the forum and hence could be labeled 'Lurkers'.

The group we label 'Browsers' ( $N=136$ , 9.1%) shows a trajectory that in many ways is similar to that of 'Lurkers'. Members allocated to this group typically enter the forum in its later stages, and show a limited number of posts. Still, their average number of posts (10.1) is almost five times higher than that of 'Lurkers' and also includes posts under the 'Girls hardcore' category. Additional to their initial registration and application to the forum, it is likely that the majority of this group has at least shown some forum browsing (yet non-communicating) activity for a relatively short period of time. Again, it seems likely that many members in this category quickly were given the status 'inactive member' for not meeting the obligatory posting frequency.

With on average 19.0 posts, the third trajectory distinguished shows a less steep decline in posting frequency than both 'Lurkers' and 'Browsers' and an average posting duration of nearly six months. In line with the overall finding that posting diversity goes up with posting frequency (Figure 4.5), we find the posting careers of this group to be more versatile in nature. Over two thirds (68%) of the members allocated to this trajectory posts under the 'Girls hardcore' topic at least once, while 26% show at least one post under the 'Boys hardcore' category. One in five members allocated to this trajectory also contributes to the 'General discussion' pages of the forum. Over half of the members in this category are registered as 'full members' by the forum administrators, suggesting that they contribute to the forum on a regular basis. We label this group, that constitutes 11.1% of the sample ( $N=167$ ), the 'cSEM interested' group.

The trajectory we label 'Escalators' ( $N=237$ , 15.8%) shows an increase in posting

frequency the longer members are active on the forum. Given the timing of their last post, were the forum not taken offline, many members in this trajectory likely would have continued to contribute to the forum. In terms of the nature of their posts, this group mirrors the 'Browser' group, in that about one in four (26.6%) of their posts falls under the 'Girls hardcore' topic. When we break down the average number of posts per topic per month active on the forum, we find no clear trend in the gravity of the cSEM as indicated by the forum topics (hardcore versus softcore). One in ten of the members allocated to the 'Escalator' group has a VIP status. As VIP status heavily depends on posting activity, the desire to reach VIP status may partially drive the escalating trajectory.

Fifth, 'Vested [cSEM community] members' (N=67, 4.5%) first become active already during the early stages of the forum's evolution. With an average of 152.4 posts, they rank among the most frequently posting groups. Nine out of ten (93%) of 'Vested members' post in the 'Girls hardcore category', while 81% contribute to the 'General discussion' topic signaling their affinity with the cSEM community as a whole. 'Vested members' are the only group of whom some members have been actively posting since the start of the forum, though their average posting career length does not differ from 'Escalators'. The large majority of members allocated to this category enjoys a 'full member' status (suggesting that they meet the posting requirements attached to this role), and 20.9% even has VIP status.<sup>2</sup>

Finally, a small (N=12), but nevertheless significant group we label 'Managers', is characterized by a posting frequency (1,636) that dwarves that of the other groups by factor 10 at the minimum. All of the 'Managers' contribute to the 'General discussion' topic (13% of their posts is dedicated to this topic), while three quarters post under the 'Information and technical safety' topic. Members in this group show the longest posting career, and half joins the forum prior to May 2013. Over half (58.3%) of the 'Managers' has an 'Administrator' or 'VIP' status.

When interpreting the trajectories, it is important to keep in mind that our data are right-censored, and that not all members could be observed for the same time period (since their first post). The 'Vested member' trajectory for example, shows a downward slope with increasing posting career length. This indicates that with time since first post on the forum, the public communication of members allocated to this group declines. This in turn may result from these members increasingly switching to private chat environments, or these members switching to other fora,

---

<sup>2</sup> A VIP status is assigned by the forum administrative team to those members who actively participate in the community by sharing their knowledge and by sharing (new and unique) cSEM. Only a small minority of forum members gets assigned this VIP status, and it might give this group access to the restricted and more private sub-fora.

perhaps in an effort to acquire new CSEM material. It could also reflect an actual decline of these members' Darkweb CSEM related activity. Given that many members allocated to this group only become active during the latter part of the forum's evolution, it must be kept in mind that the estimates for the posting trajectory for this trajectory are based on a decreasing number of members. Hence, the latter part of the trajectory increasingly depicts the trajectory of members that were among the first to enter the forum.

Finally, to examine the association between the period in the forum's evolution, and the distribution of members' posting trajectories, we cross-tabulated group membership by a variable indicating whether these trajectories were initiated during the 'start-up' period or during the 'fully functional' period. Fisher's exact test ( $p < 0.001$ ) revealed a significant association between group membership and period, with 'Lurkers' making up a larger proportion of members during the 'fully functional' period. Given the low number of posts for this category, this is unlikely to be merely an artefact of the censoring of the data.

**Table 4.4 Descriptives per trajectory group**

|                                       | Lurkers | Brow-<br>sers | CSEM<br>interes-<br>ted | Escala-<br>tors | Vested<br>mem-<br>bers | Mana-<br>gers | Brown-<br>Forsythe | Sign. | Welch   | Sign. |
|---------------------------------------|---------|---------------|-------------------------|-----------------|------------------------|---------------|--------------------|-------|---------|-------|
| <b>N</b>                              | 883     | 136           | 167                     | 237             | 67                     | 12            |                    |       |         |       |
| <b>%</b>                              | 58.8    | 9.1           | 11.1                    | 15.8            | 4.5                    | 0.8           |                    |       |         |       |
| <b>month first active</b>             | 39.92   | 38.57         | 38.49                   | 37.63           | 37.07                  | 26.92         | 12,607             | ***   | 12,841  | ***   |
| <b>month last active</b>              | 40.01   | 40.51         | 44.46                   | 48.25           | 47.67                  | 47.67         | 194,321            | ***   | 608,732 | ***   |
| <b>duration</b>                       | 0.10    | 1.93          | 5.96                    | 10.62           | 10.60                  | 20.75         | 222,875            | ***   | 546,098 | ***   |
| <b>diversity<sup>a</sup></b>          | 0.17    | 0.43          | 0.50                    | 0.58            | 0.62                   | 0.70          | 136,531            | ***   | 123,203 | ***   |
| <b># members posting</b>              |         |               |                         |                 |                        |               |                    |       |         |       |
| <b>CSEM general<sup>b</sup></b>       | 0.94    | 0.94          | 1.00                    | 0.99            | 1.00                   | 1.00          |                    |       |         |       |
| <b>girls hardcore</b>                 | 0.08    | 0.54          | 0.68                    | 0.78            | 0.93                   | 0.83          | 195,028            | ***   | 275,673 | ***   |
| <b>general discussion<sup>b</sup></b> | 0.03    | 0.26          | 0.20                    | 0.41            | 0.81                   | 1.00          |                    |       |         |       |
| <b>boys hardcore</b>                  | 0.03    | 0.19          | 0.26                    | 0.41            | 0.60                   | 0.83          | 55,705             | ***   | 64,728  | ***   |
| <b>girls softcore</b>                 | 0.03    | 0.26          | 0.31                    | 0.50            | 0.66                   | 0.75          | 65,383             | ***   | 80,723  | ***   |
| <b>restricted areas</b>               | 0.00    | 0.01          | 0.04                    | 0.12            | 0.43                   | 0.67          | 28,835             | ***   | 21,592  | ***   |
| <b>boys softcore</b>                  | 0.01    | 0.09          | 0.17                    | 0.27            | 0.42                   | 0.58          | 27,758             | ***   | 33,163  | ***   |

|                                         | Lurkers | Brow-<br>sers | CSEM<br>interes-<br>ted | Escala-<br>tors | Vested<br>mem-<br>bers | Mana-<br>gers | Brown-<br>Forsythe | Sign. | Welch  | Sign. |
|-----------------------------------------|---------|---------------|-------------------------|-----------------|------------------------|---------------|--------------------|-------|--------|-------|
| <b>information and technical safety</b> | 0.06    | 0.04          | 0.08                    | 0.12            | 0.42                   | 0.75          | 20,797             | ***   | 13,285 | ***   |
| <b>mean # posts</b>                     |         |               |                         |                 |                        |               |                    |       |        |       |
| <b>total</b>                            | 2.07    | 10.10         | 18.96                   | 38.08           | 152.42                 | 1636.17       | 5,747              | ***   | 62,174 | ***   |
| <b>CSEM general</b>                     | 1.61    | 4.40          | 7.15                    | 14.77           | 43.67                  | 544.58        | 2,536              |       | 40,374 | ***   |
| <b>girls hardcore</b>                   | 0.17    | 2.43          | 3.71                    | 10.14           | 44.24                  | 220.58        | 9,398              | ***   | 52,710 | ***   |
| <b>general discussion</b>               | 0.07    | 0.73          | 1.95                    | 2.93            | 11.10                  | 220.00        | 3,432              | **    | 10,121 | ***   |
| <b>boys hardcore</b>                    | 0.07    | 0.81          | 2.72                    | 3.70            | 22.49                  | 133.33        | 4,360              | **    | 17,775 | ***   |
| <b>girls softcore</b>                   | 0.04    | 0.96          | 1.47                    | 3.32            | 15.52                  | 116.92        | 2,958              |       | 15,880 | ***   |
| <b>restricted areas</b>                 | 0.00    | 0.10          | 0.51                    | 0.97            | 6.79                   | 95.00         | 4,116              | **    | 4,981  | ***   |
| <b>boys softcore</b>                    | 0.03    | 0.57          | 1.32                    | 2.01            | 7.34                   | 224.58        | 1,724              |       | 9,033  | ***   |
| <b>information and technical safety</b> | 0.08    | 0.11          | 0.11                    | 0.24            | 1.25                   | 81.17         | 1,198              |       | 2,434  | **    |

\*  $p < 0.1$ ; \*\*  $p < 0.05$ ; \*\*\*  $p < 0.01$

a Diversity computed across entire posting career, only for careers with at least two posts

b Robust test of equality of means can not be computed as at least one group has zero variance

## 4.4 Discussion

First, the current study quantitatively examined the evolution of a Darkweb forum dedicated to the exchange of CSEM, and supportive of adult-child sexual contact in general. This particular forum was active for over four years before it was shut down by law enforcement. During the latter 16 months the forum was operational, it morphed from a relatively secure and hidden forum, into an open forum each month attracting hundreds of new members and members adding between 20,000 and 30,000 posts to the forum website. A development that seemed instigated by a change in the forum's management, and that likely contributed to the forum's eventual demise. Though selected in part because of its size and focus and therefore not representative for the total population of Darkweb CSEM fora, these figures help to fathom the scope of the problem of online CSEM.

At the same time, these figures add nuance. While viewing and downloading CSEM are clearly illegal, and the continuous demand for CSEM creates a similarly continuous supply, the reverse also seems true, such that the sheer presence of CSEM on the internet tempts a serious number of individuals to enter a CSEM dedicated Darkweb

forum out of curiosity rather than out of a fully developed sexual interest in under-aged children. For over one third of the membership of the forum under scrutiny here, their posting is limited to the mandatory post needed to (temporarily) gain access to the CSEM forum.

Next, we took both Quayle and Taylor's (2003) model of problematic internet use, and Lanning's (2001) typology of online CSEM offenders as theoretical vantage points, to further scrutinize variation in the different dimensions of the longitudinal sequence of individual's forum posting behavior. Motivated by curiosity and opportunity, situationally motivated normal adolescents/adults were predicted to show a late onset (with regard to the forum's establishment, rather than to the offender's calendar age), low frequency and short duration of their posting 'career' (hypothesis 1). Corroborating the findings on the skewness in individual posting frequency, results of the GBTM identify a trajectory, comprising over half of the forum members, that is characterized by exactly these features and whose posting 'career' on the forum seems to end more or less where it begins. The posting behavior of these 'Lurkers' therefore fits with what could be expected from Lanning's 'Normal adolescent/adult' type.

Preferentially motivated pedophiles are expected to show posting careers that are early onset, high frequency and long duration, and besides posts on sexual topics, contain posts indicating an interest in CSEM community building (hypothesis 3). The trajectory we labelled 'Vested members' seems to best fit Lanning's 'Pedophile' type. These forum members are frequent contributors to the forum's content, and regularly submit posts to both sexual topics, and topics of a more 'social' nature. These members' posting trajectory and formal forum status signal their vested interest in the forum and the CSEM community as a whole. Given their most recent activity on the forum is temporally close to the forum's closure, 'Vested members' would likely to have continued their offending given prolonged opportunity.

Both the 'Morally indiscriminate' and the 'Diverse' offender type were predicted to show a pattern of posting behavior falling somewhere in between that of 'Normal adolescents/adults' and 'Pedophiles' (hypotheses 2 and 4). Two trajectories, those we labeled 'Browsers' and 'CSEM interested' meet these criteria. Within the limits of the available data however, neither of these trajectories shows clear signs of a more diverse sexual interest compared to the other trajectories. Members on the 'CSEM interested' trajectory are also socially active on the forum, which does not fit either the indiscriminate or diverse type, positioning them closer to 'Vested members' in that respect. Additional information about members online pornography use (e.g. activities on different legal and illegal pornographic websites) collected during police investigations, or content analysis of their forum posts, could help to differentiate indiscriminate from diverse online CSEM offenders.

The trajectory we labelled ‘Escalators’ combines a late onset with an increasing posting frequency. As with the ‘Vested members’ we find no reason to assume these ‘Escalators’ were to discontinue their forum behavior any time soon had the forum not been shut down. The posting trajectory displayed by these members fits that of Lanning’s ‘Latent offender’ type (hypothesis 5), with the exception that members of the escalating trajectory do not engage much in the ‘General discussion’ topic. Hence, this trajectory seems to better fit the disinhibitory effect of merely accessing cSEM described by Quayle and Taylor’s (2003) model of problematic internet use.

Finally, our GBTM analysis distinguishes a group of forum members whose posting behavior diverges widely from that of the other members in terms of onset, frequency and duration, and does not seem to readily fit any of the types in the Lanning typology. We labeled this group ‘Managers’ because their posting behavior does not seem to primarily result from their own sexual interests, but rather from the managerial tasks these members have taken upon themselves in order to keep the cSEM forum up and running. In some ways, this trajectory mirrors Lanning’s (2001) ‘Profiteer’ type, or Elliott and Beech’s (2009) ‘Commercial exploitation’ type, in that being an administrator of a Darkweb forum is perceived as ‘a full-time job’, requiring much more forum activity than that required to fulfill private goals. Importantly however, while supervising a Darkweb cSEM forum may provide ‘Managers’ with certain benefits, these benefits do not seem to include monetary profits. Like ‘Vested members’ therefore, ‘Managers’ extensive involvement with the cSEM community, is likely driven by a definite sexual preference for children characteristic for the ‘Pedophile’ offender type (Lanning, 2001).

#### **4.4.1 Limitations**

Linking the observed posting trajectories to existing offender typologies rests on the assumption that posting behavior reflects member’s motivation and sexual interest. Other factors may however help shape members’ forum behavior, like the availability of material that suits members’ sexual interests, the user friendliness of the forum, the responsiveness of the forum’s management and fellow members to technical questions or substantive requests, or their willingness or ability to submit themselves to the posting regime of the particular forum. It should also be kept in mind that individuals may simultaneously visit and be member of more than one Darkweb cSEM forum, and that their behavior may differ on each of these fora. Reconstructions of online behavior are therefore never completely accurate measures of sexual interests and motivation (Brennan & Hammond, 2017; Fortin & Proulx, 2019).

Aside from this more general caveat, a number of limitations specific to the current study need mentioning. First, as mentioned in the method section, the available data

only covered publicly posted forum communications and we have no way of estimating the size and nature of any private communications going on between members. Private communications however typically initiate from public interactions, so, while likely underestimating the frequency of total forum communication, public posts may still accurately reflect the topics discussed. Furthermore, only when the ratio between public and private communications were to differ between member types, would this influence the rank ordering of the trajectories distinguished.

Second, unlike previous studies (Fortin & Proulx, 2019; Taylor et al., 2001), ours did not include an assessment of the actual CSEM exchanged or collected through the forum's website. Rather, we relied on categorizations made by the forum's administrators to typify the topics of the posts analyzed. While our findings are in line with results from previous studies, for example with regard to the popularity of CSEM depicting underaged girls over that of CSEM depicting underaged boys (Fortin & Proulx, 2019), the crude distinction between 'softcore' and 'hardcore' may have limited our ability to detect trends in the severity of members posting careers, and hence adequately test assumptions regarding habituation and escalation of offending behavior over time.

Third, our data were right-censored. This means that especially for those becoming first active on the forum during the latter part of the observation window, the observed trajectory may not reflect the entire posting career. While GBTM is designed to handle missing data, adding measurements – i.e. additional months – may alter the shape of the trajectories identified. Hence, we remain uncertain of the extent and nature of continued forum activity for the vested and escalating groups. Our view of the cycle of managerial turnover is also limited. That said, for the most prevalent trajectories the time between the last known post and the forum being taken down is such that we can safely conclude, especially against the background of this particular forum's mandatory contribution policy, that many members following these trajectories are no longer active participants in the forum.

Finally, distinguishing trajectories using GBTM is best viewed as a way of reducing the complexities of observational data by collapsing these complexities within a limited number of trajectories. While these trajectories may aid further interpretation of Darkweb CSEM members forum behavior, their theoretical relevance depends on the extent to which these online communication patterns can be linked to theoretically derived variables that may explain both their prevalence and developmental pathway. To further assess the bearing these trajectories have on the Lanning (2001) typology for instance, would require research that combines behavioral measures – like forum posting – with measures of sexual motivation. Retrospective, longitudinal analysis of online offenders' CSEM collections, matched with survey measures of sexual interest,

treatment file information, and records on offenders' previous sexual and nonsexual transgressions, would be a fruitful avenue of future research in this respect.

#### **4.4.2 Future research avenues and implications**

Despite these limitations, the current study adds to a budding literature analyzing the online behavioral patterns of those who use the internet to commit sexual offenses (e.g. Brennan & Hammond, 2017; Hammond et al., 2009; Taylor et al., 2001). While various typologies of online sex offenders have been offered, few offer the detail needed to derive precise hypotheses on the behavioral patterns to be expected for each of these types. The current study, and other studies applying a criminal career paradigm to online CSEM offending (Fortin & Proulx, 2019; Westlake & Bouchard, 2015), will probe theorists of sexual offending to further refine their explanations and incorporate concrete and testable expectations in their models. While the current analysis reconstructed forum members' communication patterns in a posterior fashion, future research could also assess the extent to which it is possible to predict members' future forum position, based on the development of their online communications. In this way, interventions could be designed aimed at curbing members' developmental pathway and preventing their online offending from spiraling out of control.

Apart from implications for future academic theory and research, the results of the current study may aid professional practice. Quantitatively charting the behaviors of online CSEM offenders can assist law enforcement in targeting specific fora or specific (groups of) forum members for further (qualitative) assessment and intervention. On the forum level, research indicates that the total volume of traffic on a forum predicts its persistence (Westlake & Bouchard, 2015). Fora showing an increase in communications, like the one studied here, therefore demand prioritization. On an individual level, member profiles can inform investigators which offenders to target for undercover operations, and on how to approach them taking into account their offending motivation. Different Darkweb forum members may also require different interventions to prevent them from future offending. Whereas situationally motivated lurkers and browsers may be deterred from CSEM offending by increasing their perceived risk of exposure and prosecution, vested members and managers – given their vested interests in the CSEM community – likely are not, or to a much lesser extent. This knowledge is not only informative to law enforcement, but also to clinical-forensic professionals in assessing offenders and offering them the most effective treatment with the aim of reducing future offending.

## Appendix

**Table A1 Criteria used for assessing GBTM model fit**

| #<br>groups | order | BIC (obs)<br>N=16,455 | BIC (ind)<br>N= 1,502 | AIC        | LL         | Estimated group probability ( $\pi_j$ ) |       |       |       |       |       |       |
|-------------|-------|-----------------------|-----------------------|------------|------------|-----------------------------------------|-------|-------|-------|-------|-------|-------|
|             |       |                       |                       |            |            | grp 1                                   | grp 2 | grp 3 | grp 4 | grp 5 | grp 6 | grp 7 |
| 1           | 2     | -16,934.74            | -16,931.15            | -16,923.18 | -16,920.18 | 100.0                                   |       |       |       |       |       |       |
| 2           | 2     | -11,682.76            | -11,674.38            | -11,655.78 | -11,648.78 | 70.2                                    | 29.8  |       |       |       |       |       |
| 3           | 2     | -11,103.13            | -11,089.96            | -11,060.73 | -11,049.73 | 20.6                                    | 64.5  | 15.0  |       |       |       |       |
| 4           | 2     | -10,879.3             | -10,861.35            | -10,821.49 | -10,806.49 | 16.1                                    | 62.0  | 4.3   | 17.6  |       |       |       |
| 5           | 2     | -10,842.25            | -10,819.51            | -10,769.02 | -10,750.02 | 11.1                                    | 16.5  | 12.4  | 55.8  | 4.2   |       |       |
| 6           | 2     | -10,809.92            | -10,782.39            | -10,721.27 | -10,698.27 | 11.2                                    | 4.4   | 12.0  | 55.9  | 1.2   | 15.3  |       |
| 7           | 2     | -10,803.4             | -10,770.72            | -10,698.98 | -10,671.98 | 11.4                                    | 3.9   | 2.9   | 55.8  | 1.2   | 15.0  | 9.8   |
| 1           | 3     | -16,485.32            | -16,480.54            | -16,469.91 | -16,465.91 | 100.0                                   |       |       |       |       |       |       |
| 2           | 3     | -11,586.84            | -11,576.07            | -11,552.16 | -11,543.16 | 70.3                                    | 29.7  |       |       |       |       |       |
| 3           | 3     | -11,097.92            | -11,081.16            | -11,043.96 | -11,029.96 | 20.3                                    | 64.9  | 14.8  |       |       |       |       |
| 4           | 3     | -10,86.69             | -10,863.94            | -10,813.46 | -10,794.46 | 17.9                                    | 15.6  | 62.0  | 4.4   |       |       |       |
| 5           | 3     | -10,867.93            | -10,839.2             | -10,775.43 | -10,751.43 | 9.0                                     | 14.1  | 61.8  | 1.9   | 13.3  |       |       |
| 6           | 3     | -10,842.79            | -10,808.08            | -10,731.0  | -10,702.0  | 8.1                                     | 10.7  | 56.4  | 1.8   | 10.5  | 12.5  |       |

Note Additional indicators of model fit (Nagin, 2005) for the 6 group model:

$2(\Delta BIC)$  approximates the logged Bayes factor, values  $> 10$  indicate the more complex model is preferred

AvePPj  $> 0.7$  for all groups (0.81; 0.76; 0.76; 0.94; 0.98; 0.79)

OCCj  $> 5$  for all groups (34.2; 67.9; 23.8; 13.0; 3281.3; 20.6)

Pj -  $\pi_j$  small for all groups (2.1; -0.1; 0.8; -2.9; 0.4; -0.5)

| Average posterior probabiliy of assignment (AvePPj) |          |          |          |          |          |          |           |
|-----------------------------------------------------|----------|----------|----------|----------|----------|----------|-----------|
| grp1prb                                             | grp2prb  | grp3prb  | grp4prb  | grp5prb  | grp6prb  | grp7prb  | 2(ΔBIC)   |
| .9917348                                            | .9828731 |          |          |          |          |          | 10,503.96 |
| .8796656                                            | .9858674 | .9324765 |          |          |          |          | 1,159.26  |
| .817657                                             | .9802669 | .8883356 | .8718029 |          |          |          | 447.66    |
| .8116903                                            | .8328345 | .779667  | .9419771 | .8973085 |          |          | 74.1      |
| .8119631                                            | .7579809 | .7639651 | .9428063 | .9761599 | .7882499 |          | 64.66     |
| .8115411                                            | .7504362 | .7405008 | .9412045 | .9710648 | .7674629 | .7290794 | 13.04     |
|                                                     |          |          |          |          |          |          |           |
| .992196                                             | .9791056 |          |          |          |          |          | 9,796.96  |
| .8800361                                            | .9857991 | .9197945 |          |          |          |          | 977.84    |
| .8633809                                            | .8185469 | .9798812 | .8977453 |          |          |          | 422.46    |
| .7946093                                            | .7617594 | .9782184 | .8797509 | .7633095 |          |          | 37.52     |
| .7757446                                            | .7637236 | .9353699 | .8592755 | .7258472 | .7191928 |          | 50.28     |

**Table A2 Results of the GBTM model fit, comparing the 10% analysis sample to the remaining 90% of the total sample**

| Forum characteristic                    | not in GBTM | in GBTM | standardized difference |
|-----------------------------------------|-------------|---------|-------------------------|
| <i>N</i>                                | 13,336      | 1,502   |                         |
| %                                       | 89.88       | 10.12   |                         |
| <b>month first active</b>               | 39.00       | 39.04   | 0.01                    |
| <b>month last active</b>                | 42.25       | 42.25   | 0.00                    |
| <b>duration</b>                         | 3.25        | 3.21    | -0.01                   |
| <b>diversity<sup>a</sup></b>            | 0.39        | 0.40    | 0.01                    |
| <b># members posting</b>                |             |         |                         |
| <b>CSEM general</b>                     | 0.96        | 0.96    | -0.01                   |
| <b>girls hardcore</b>                   | 0.33        | 0.34    | 0.03                    |
| <b>general discussion</b>               | 0.16        | 0.17    | 0.05                    |
| <b>boys hardcore</b>                    | 0.15        | 0.16    | 0.02                    |
| <b>girls softcore</b>                   | 0.18        | 0.19    | 0.01                    |
| <b>restricted areas</b>                 | 0.06        | 0.05    | -0.05                   |
| <b>boys softcore</b>                    | 0.09        | 0.10    | 0.04                    |
| <b>information and technical safety</b> | 0.09        | 0.09    | -0.01                   |
| <b>mean # posts</b>                     |             |         |                         |
| <b>total</b>                            | 28.12       | 30.12   | 0.01                    |
| <b>csem general</b>                     | 10.87       | 10.77   | 0.00                    |
| <b>girls hardcore</b>                   | 6.03        | 6.07    | 0.00                    |
| <b>general discussion</b>               | 3.21        | 3.04    | 0.00                    |
| <b>boys hardcore</b>                    | 2.39        | 3.07    | 0.03                    |
| <b>girls softcore</b>                   | 1.90        | 2.43    | 0.02                    |
| <b>restricted areas</b>                 | 1.75        | 1.28    | -0.02                   |
| <b>boys softcore</b>                    | 1.24        | 2.65    | 0.04                    |
| <b>information and technical safety</b> | 0.75        | 0.81    | 0.00                    |

a Diversity computed across entire posting career, only for careers with at least two posts



CHAPTER 5

# EVEN “LURKERS” DOWNLOAD: THE BEHAVIOR AND ILLEGAL ACTIVITIES OF MEMBERS ON A CSAM TOR HIDDEN SERVICE

***This chapter has been published as:***

Van der Bruggen, M., Van Balen, I., Van Bunningen, A., Talens, P., Clapp, K., & Owens, J. (2022). Even “lurkers” download: The behavior and illegal activities of members on a child sexual exploitation Tor Hidden Service. *Aggression and Violent Behavior*, 67. <https://doi.org/10.1016/j.avb.2022.101793>

***“In loving memory of Special Agent Daniel Alfin, without whom,  
this research would not have been possible.”***

## **Abstract**

Knowledge about online child sexual exploitation (CSE) offenders mostly remains limited to offender populations known by the criminal justice system. Because of its hidden and anonymous nature, knowledge on those offenders active on the Darkweb is especially scarce. For the current study, researchers had access to a unique dataset of member communication on a Darkweb CSE website, as well as members' virtual movements (or clicks) across the site, regardless of being verbally active or not. This offered a unique opportunity to establish behavioral patterns of members who were unaware that they were being observed. This paper summarizes the results of a descriptive analysis of the growth of member count, the frequency with which members were online, and detailed member behavior such as their activity on certain sub-forums and their downloading activity. Main findings include that although only 3.4% of the members were communicatively active, the vast majority of 93.6% of members downloaded CSE material. Results indicate that regardless of being verbally active, most members do engage with the site's content, and thus, effectively impact the CSE community. This has important implications for law enforcement practice, which will be discussed.

## **5.1 Introduction**

The distribution of online child sexual exploitation (CSE) material is a serious crime, with severe societal consequences. Combining this with the increased opportunities, accessibility and anonymity of the internet, it is only logical that online CSE has attracted increased attention from researchers from various disciplines in recent years. Examples from psychological research include studies exploring differences between online and contact offenders (e.g. Babchishin et al., 2015; Owens et al., 2016), the risk that online offenders commit additional crimes against children (past, present, or future), including contact offences and the production of CSE material (e.g. Seto & Eke, 2005; Seto & Eke, 2015), and the evaluation of treatment approaches (e.g. Seto & Ahmed, 2014). From a criminological perspective, several studies have aimed to classify online CSE offenders based on type of and motivation for offending (e.g. Lanning, 2010; Merdian et al., 2013; Shelton et al., 2016). What characterizes many of these prior studies is the fact that they were conducted on offender populations known by the criminal justice system or by healthcare professionals. Much less is known about those offenders that remain active in online CSE communities for longer periods of time but may not (yet) be caught.

Rather than focusing on individual offenders, their motivation and risk, or aiming to uncover the more hidden groups of offenders, another strand of research focuses on the platforms and networks facilitating online CSE offending instead. For example, Steel (2009) quantified and described the nature of CSE material exchanged on a peer-to-peer platform by analyzing CSE-related querying and traffic on those platforms. Other studies focused on the social and interpersonal aspects of offenders who gather and communicate online, the normalizing aspect of child abuse, and pro-offending attitudes (O'Halloran & Quayle, 2010; Prichard et al., 2011). Studies in these areas conclude that the lack of reinforcement of social norms leads to a feeling of freedom to break these norms within online CSE communication spaces (Rimer, 2017). Finally, Canadian researchers took a strict network perspective with CSE websites as the unit of analysis, considering the online CSE network as a large virtual community connected through hyperlinks (Westlake & Bouchard, 2016). They identified certain “key-player websites” based on content severity and connectivity to other CSE websites, and determined that their removal would result in a loss of network capital (Westlake et al., 2011). From an evolutionary point of view, Westlake and colleagues further suggested that popular, central, and larger websites are the most persisting and have the greatest chances of survival (Westlake & Bouchard, 2015); however acknowledging websites still demonstrate a vulnerability to attack strategies that can cause disruption and network fragmentation (Joffres et al., 2011).

An underlying factor that characterizes most of these studies is the fact that they were conducted on Clearnet platforms. Much less is known about the more hidden groups of offenders active on the Darkweb, the encrypted part of the internet that exists at hidden levels outside of the observable internet and that is only accessible through specific software (the best known example being TOR). Much of the CSE offending on the Darkweb takes place on websites called “hidden services” that are only accessible via the TOR network, and structurally consist of layers of forums and sub-forums. Research on CSE offender behavior would benefit from additional insight regarding the manner in which the Darkweb’s anonymous infrastructure facilitates increased trafficking and secure downloading of CSE material.

The very limited research previously conducted on Darkweb CSE offending (e.g. Fonhof et al., 2018; Van der Bruggen & Blokland, 2021), is based on the communication occurring on the public areas of Darkweb CSE websites, and thus solely covers members that are communicatively active and visible on the site. Hardly anything is known about the so-called “lurkers”, those members of online communities that observe but do not actively participate (in the form of posting messages within the public environments of the website). It is this group that contains the truly hidden CSE offenders on the Darkweb.

For the current study however, the researchers had access to a unique and unprecedented dataset of a CSE TOR hidden service. This dataset not only archived member communication exchanged during the entire time the site was online, but also captured all member movements (or clicks) behind the screen/keyboard for a specific and shorter timeframe of interest. Therefore, activity such as clicking on internal and external links, regardless of members being communicatively active or not, was available for analysis. This offered a unique opportunity to establish behavioral patterns of members who were unaware that they were being observed and therefore showed their natural behavior. This paper summarizes the results of a descriptive analysis of the proportion of members that were not verbally active, the frequency with which they were online, on which sub-forums they were most active, and their attempts to download CSE material. The aim of the current paper is to describe and compare members' movement and activity (clicks), offering greater insight into behavioral characteristics of the "average" member on CSE hidden service communities on TOR. The results suggest that in addition to those members who visibly communicate, the vast majority of lurkers are also active and motivated members who (attempt to) download CSE material. Thus, the current study provides a more comprehensive picture of CSE offending behavior on the Darkweb.

### **5.1.1 Darkweb CSE hidden services and lurking**

The ability to freely access relatively unique and new CSE material in large quantities and the desire to be part of a community of like-minded others in relative anonymity, has recently led to large numbers of online CSE offenders relocating to the Darkweb (Finklea, 2017; Van der Bruggen & Blokland, 2021). Darkweb CSE hidden services, also called forums, are similar to forums on the Clearnet, with their homepage typically listing a number of sub-forums, under which members can navigate to and submit messages or referrals to a multitude of sexually abusive material depicting children. These messages result in threads that can evolve into long-running discussions between countless members. Sub-forums often refer to environments where hyperlinks to content of a certain sexual interest (i.e. age and/or gender of the depicted children, the severity of the material, or the type of sexual act) should be placed. Threads in such sub-forums involve communication and negotiation about the exchange of the CSE material, and extensive discussions about members' sexual preferences, fantasies, and experiences. However, popular sub-forums also provide locations where members can access information about the hidden service's rules and regulations, (technical) safety, and law enforcement operations and evasion techniques, which offer education and guidance among members. Darkweb CSE hidden services often have a hierarchical order: members have a certain status assigned to them (such as regular mem-

ber, moderator, or administrator), depending on their activity, popularity or formal responsibility. It is not uncommon for members with a higher status to have access to certain restricted or hidden sections of the forum, for example consisting of “administrator-only” information or more unique and/or newly produced CSE material (Bartlett, 2014; Van der Bruggen & Blokland, 2021).

After having registered with a nickname and password to gain access to the hidden service, not all members portray the same level of activity. Some members are significantly more active within the community, communicate regularly about topics relevant to the forum’s continuity and may even have a role in the technical development and management (with or without a formal status). More commonly, members may be more or less active, but their communication centers on certain topics related to their sexual experiences and fantasies and the exchange of CSE material. Finally, there are those members that “solely” use the website to browse around seeking access to and potentially obtaining CSE content, yet who do not communicate or contribute material. This final group is often characterized as “lurkers”. Although this sub-group of members may not actively contribute to the community with regards to the uploading of CSE material or communication with others (such as explicitly encouraging others to offend against children and produce new material), these so-called “lurkers” actively read the postings and their mere presence on the site creates and facilitates the demand for more CSE material.

Although to date there is no research on lurking on CSE hidden services specifically, previous academic research has been conducted on lurking on other online platforms and social media communities. From this research, it is evident that lurking is very normal internet behavior, with lurkers constituting a significant proportion of approximately 90% of all users active on the platforms studied (Gong et al., 2015; Mousavi et al., 2017; Nonnecke & Preece, 2000; Tagarelli & Interdonato, 2013). This suggests that not paying attention to these users could lead to a misinterpretation of the overall population and their behavior (Gong et al., 2015).

Historically, lurkers were negatively seen as “free-riders” benefiting from the contributions of the community without offering anything in return, arguably because online platforms are dependent on collaboratively generated content by their users. However, more recently lurkers have been categorized as harmless, curious and passive participators (Cranefield et al., 2015; Tagarelli & Interdonato, 2013). Through their presence and browsing activity, the forum’s posts and threads receive increased numbers of views, so even indirectly lurkers facilitate the content to reach a larger audience. Moreover, lurkers may have good reasons to stay silent, such as not feeling the need to post, privacy and safety concerns, poor system usability, user friendliness, and improving their understanding of the community etiquette before starting to par-

ticipate (Preece et al., 2004). In fact, in some cases lurking may even be beneficial, as some forms of active communication may be deemed negative and undesirable, and it may even harm the community (Lutz & Hoffmann, 2017; Tagarelli & Interdonato, 2013). Furthermore, lurkers may be active participators in other, more restrictive/private areas of the site or on entirely different sites, such as on a separate personal message systems or on other but similar online platforms. Lurkers may, therefore, still have important ties with influential fellow members or with the larger network (Cranefield et al., 2015; Tagarelli & Interdonato, 2013). Along these lines, Cranefield et al. (2015) discussed “follower-feeders”, the online followers and offline leaders, or invisible members who only communicate privately with influential and trusted others and who play a brokering role in transferring knowledge between contexts within the broader ecosystem. Finally, lurkers may ultimately break their silence at some point, for example, to share information or to update other users about their personal life (Gong et al., 2015).

From an emotional perspective, rather than viewed as unimportant or harmless users, lurkers are individuals with interests and consume the content related to those topics that interest them (Gong et al., 2015). Observing what other members do resembles a process of vicarious learning about the community and topic of interest, and it affects attitudes and future behavior (Bozkurt et al., 2020; Mousavi et al., 2017). The cognitive and emotional investment made in their online presence, as well as their feelings of belongingness to the community may be as significant as for active users (Lutz & Hoffmann, 2017; Mousavi et al., 2017). To this point, research conducted on online brand communities revealed that lurkers were just as valuable members as their more active posting counterparts, and similarly derived their social identity from their membership of the online community (Mousavi et al., 2017).

Taken together, aside from the exchange of CSE material, a main interest of a CSE hidden service is to have public influence (Van der Bruggen & Blokland, 2021), and lurkers create just that, which means that they are of value without being active posters. Where previous research on online communities has mainly focused on observable acts of communication and content creation, future research would benefit from more incorporation of hidden concepts such as motivation and intent (Bozkurt et al., 2020; Lutz & Hoffmann, 2017; Mousavi et al., 2017). Such concepts could be inferred by members’ movements within the online communities under consideration (for example, time spent online, numbers of pages visited, and downloaded content) and their activities in the broader and external online and offline ecosystem (Mousavi et al., 2017).

## 5.2 Methods

### 5.2.1 Data and sample

The data used for the current study were extracted from a Darkweb CSE hidden service, which was only available to members via the TOR network. The areas in which discussions took place and content was shared were divided into forum and sub-forum environments, predominantly focusing on victim gender (boys versus girls), and severity of content (hardcore versus softcore CSE material). Additionally, there were environments for certain sexual acts and fetishes, and administration-related security and information environments. During the timeframe when data were collected for analysis, this hidden service amassed activity in 13 forums and 55 sub-forums, within which members could create and title their own threads for discussions and the exchange of CSE material. Members who posted visual material typically provided a thread title and a preview image associated with the depicted content that could be downloaded with the embedded hyperlink. By clicking the link, the downloading member would then be referred to an external hosting website where the content could be downloaded. The overall site would be considered an “open board”, as registered members were not required to contribute themselves in order to gain access to the CSE material. Finally, this hidden service was online for a period of less than a year, which can be considered a relatively short period of time compared to other CSE hidden services. However, because this hidden service had the largest number of members and activity at the time, there was no shortage of data for extensive analyses.

The authors had access to two separate datasets for analysis. Dataset 1 contained registration-, member-, and communication-related data (public posts as well as private messages) from August 2014 to March 2015. In other words, this included the written communication data regarding the entire 8-month period that the hidden service was online. This sample consisted of a total of 417,438 members.<sup>1</sup> Dataset 2 included all members’ movements (or clicks) and activity within a specific two-week timeframe in early 2015 (specifically between February 20 and March 4, 2015), during which time the hidden service was monitored by a federal law enforcement agency. This sample consisted of a total of 97,178 members who logged in at least once during this two-week timeframe. In total, approximately one million logins were captured.

### 5.2.2 Design

The main aim of the current study was to determine and describe all forum activity

---

<sup>1</sup> Because an individual could register with multiple accounts, the researchers acknowledge that this number is an approximation, as there is no way to know how many unique individuals this number represents.

from the CSE hidden service data available, including that of members that were not verbally active via public posts. This was operationalized by the term “behavior flow”, defined by the authors as the way in which members traverse and interact with the website. More specifically, behavior flow is used to define the logged/captured clicks of a member, visiting various internal or external hyperlinks during a single session on the website. This can, but does not necessarily, include verbal communication by means of making a post, as well as all (usually hidden) forum behavior extending beyond what is visible on the site. Examples of this hidden behavior include actively navigating to a certain forum, trying to gain access to a certain sub-forum, or (making the attempt) to download a file.<sup>2</sup>

Three dependent variables were measured: 1) the average time spent on the hidden service, 2) the frequency of visiting, and 3) the activities undertaken during a visit (sub-forum visits and (attempted) downloads). An activity was recorded when a member clicked on an internal link to a certain sub-forum or on an external link to the CSE material in an attempt to download it to his or her personal computer. For the current descriptive analysis, univariate descriptions with measures of central tendency were used.

## 5.3 Results

### 5.3.1 Basic analyses: Dataset 1

In order to illustrate member behavior and describe the “average” member, a number of basic descriptive analyses were conducted. To do so, initially the first dataset (registration-, member-, and communication data from all registered members regarding the total 8-month period that the hidden service was online) was used. In order to assess the hidden service’s development and growth, an evaluation of the start of membership (using members’ first logon time on the website) was conducted. The results illustrate that only the administrator registered on the hidden service in early August 2014. However, on the first day that the website became publicly available, an additional 321 members registered with a member profile. Within the first week, a total of 6,968 profiles were registered.

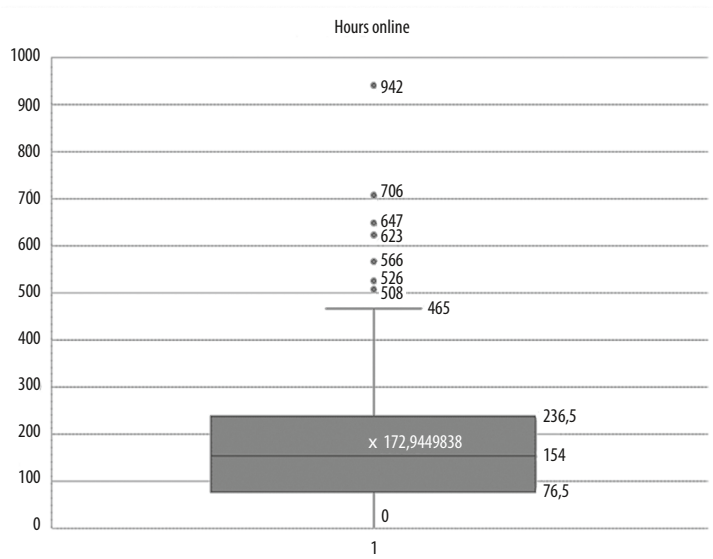
Further examination of the registered profiles revealed that only a small minority, 3.4%, of all members were verbally active at some point during the 8-month period that the site was online (14,088 of 417,438 members); the remaining 96.6% did not post

---

<sup>2</sup> Researchers are using the term “attempted download” because it represents a member clicking on a hyperlink to attempt to download a file. Given the data available to researchers, there was no way to confirm whether the download was completed or not, or if the file associated with the link was still available at the time of the click.

any message on the public areas of the site.<sup>3</sup> On average, members were online for 7.8 hours in total, with a variation of 0 to 942 hours. An important reason for this great variation in total logon time is the fact that this distribution included several outliers of members who were online for over 500 hours, with the administrator being online the longest (942 hours).<sup>4</sup> On the contrary, there was a larger number of members who were only online briefly. More than half of all members (55%, or 225,969 members) were online for a total of less than 1 hour during the total 8-month timeframe the hidden service was online. In order to gain more insight into the distribution, the median was calculated (Figure 5.1). This analysis revealed that 416,992 members (or 99% of the member population) were online less than the median time of 154 hours. Finally, just under 6% of members were not only online for less than 1 hour, but apparently only registered on the website and went offline shortly after that and never came back. A noted caveat to this finding is the possibility that some of these members may have registered right before the site was shut down, and therefore did not have the chance to come back online.

**Figure 5.1** Boxplot of median time online in hours



3 Members may however have been active in the non-public areas of the hidden service (such as private or hidden areas, or via personal messages). These areas were not taken into account in this analysis.

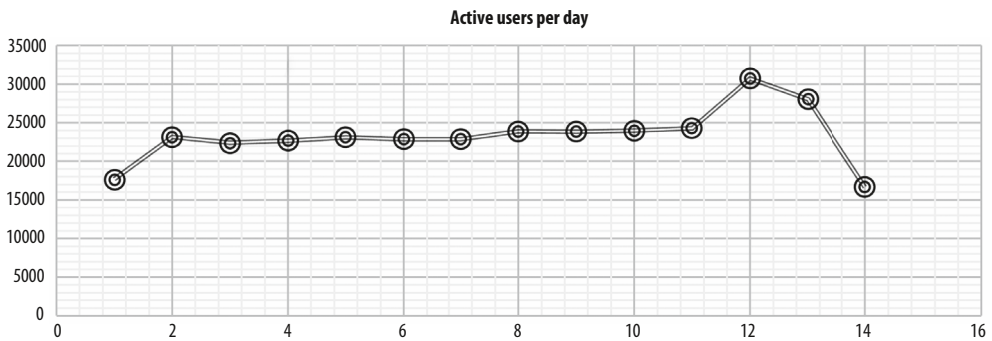
4 Being online means that a member was logged on to the website for the number of hours stated in this paper. This does not necessarily mean that a member has shown activity (in the form of posting content) within this time-frame.

In order to calculate the timeframe during which members were online, the period between when a member created his profile (“create profile”) and the last time a member was online (“last seen online”) was measured. Findings indicate that the “average” member was active on the CSE site for a duration of 2-3 months (84 days), with a total logon time of 10-12 hours. This is equivalent to approximately 0.13 hours per day, or just under 1 hour a week. There were also some noted outliers of members who were online very frequently.

### 5.3.2 Behavior flow analyses: Dataset 2

In order to demonstrate in more detail how members interact within the CSE hidden service, the second dataset with logged/captured clicks of a registered member (behavior flow) on the site was analyzed. Therefore, the following results refer to the limited two-week timeframe in which a total of 97,178 members engaged in any activity on the site. Figure 5.2 illustrates the number of active members per day within the two-week timeframe.

**Figure 5.2 Scatterplot of the count of active members per day within the two-week timeframe**



Members were divided into two categories:

1. Registered members, who were present on the hidden service more than once, who visited various forums and sub-forums, and who had at least one download (attempt). This comprised a total of 90,943 members (93.6%).
2. Registered members, who were present on the hidden service more than once, who visited various forums and sub-forums, but did not (attempt to) download. This comprised a total of 6,235 members (6.4%).

#### 5.3.2.1 Members’ sub-forum activity and surfing behavior

Because most members had no verbal activity on the site, their behavior flow was the only data available. Therefore, these members’ activity within the 55 sub-forums was mapped.

Among all 97,178 members within the two-week timeframe analyzed, a total of 21,967,663 individual logged activities of behavior flow (or unique clicks) was measured (see also Table 5.1). Results indicated that each member made an average of 226 clicks during their time on the site. From this total number of clicks, the percentage of clicks per sub-forum was calculated, and the number of unique members located within those sub-forums was documented. These results are displayed in Table 5.1. The sub-forum “Girls Hardcore” had the highest volume of logged activity, with a total of 73,468 visits from unique forum members<sup>5</sup>, and 29.3% of the total volume of logged forum activity. The top five sub-forums with the highest volume of behavior flow (excluding sub-forums with identical titles) were: Girls Hardcore, Girls, Preteen Girl, Jailbait Girl, Family – Incest.

**Table 5.1 Total number of logged clicks and members in the various sub-forums (N = 55)**

| Sub-Forum                     | Total number of logged clicks | Logged clicks: % of total | Total number of unique members |
|-------------------------------|-------------------------------|---------------------------|--------------------------------|
| 6 (Girls HC)*                 | 6,439,786                     | 29.31%                    | 73,468                         |
| 16 (Girls)                    | 3,223,791                     | 14.68%                    | 57,846                         |
| 56 (Girls)                    | 2,030,077                     | 9.24%                     | 36,473                         |
| 10 (Girls HC)                 | 1,417,450                     | 6.45%                     | 47,980                         |
| 41 (Preteen – Girl)           | 1,090,865                     | 4.97%                     | 44,332                         |
| 40 (Jailbait – Girl)          | 927,187                       | 4.22%                     | 38,413                         |
| 17 (Girls SC/NN)              | 832,041                       | 3.79%                     | 30,828                         |
| 26 (Family Play Pen – Incest) | 791,721                       | 3.60%                     | 34,214                         |
| 8 (Girls)                     | 702,891                       | 3.20%                     | 33,069                         |
| 19 (Girls SC/NN)              | 610,794                       | 2.78%                     | 24,308                         |
| 33 (Vintage)                  | 403,194                       | 1.84%                     | 13,952                         |
| 7 (Boys HC)                   | 388,001                       | 1.77%                     | 20,201                         |
| 25 (Toddlers)                 | 363,373                       | 1.65%                     | 16,096                         |
| 23 (Request)                  | 317,855                       | 1.45%                     | 29,871                         |
| 22 (General Discussion)       | 315,688                       | 1.44%                     | 24,507                         |
| 45 (Zoo)                      | 193,070                       | 0.88%                     | 16,515                         |
| 34 (Voyeur)                   | 182,769                       | 0.83%                     | 14,213                         |
| 31 (Peeing)                   | 157,458                       | 0.72%                     | 10,000                         |
| 30 (Bondage)                  | 126,210                       | 0.57%                     | 12,651                         |
| 51 (Español)                  | 114,568                       | 0.52%                     | 7,575                          |

5 By unique forum members, the researchers refer to the fact that this number does not include double visits. Again, because an individual could register with multiple accounts, the researchers acknowledge that it is unclear how many unique individuals in real life this number represents.

| Sub-Forum                                                 | Total number of<br>logged clicks | Logged clicks:<br>% of total | Total number of<br>unique members |
|-----------------------------------------------------------|----------------------------------|------------------------------|-----------------------------------|
| 32 (Artwork)                                              | 92,514                           | 0.42%                        | 7,353                             |
| 11 (Boys HC)                                              | 87,517                           | 0.40%                        | 10,650                            |
| 52 (Deutsch)                                              | 82,593                           | 0.38%                        | 5,426                             |
| 38 (Chubby)                                               | 79,460                           | 0.36%                        | 9,008                             |
| 24 (Panties, nylons, spandex)                             | 77,588                           | 0.35%                        | 8,115                             |
| 58 (Русский – Russian)                                    | 72,870                           | 0.33%                        | 5,522                             |
| 37 (Non-fiction)                                          | 64,262                           | 0.29%                        | 7,130                             |
| 53 (Português)                                            | 60,151                           | 0.27%                        | 3,706                             |
| 5 (Boys)                                                  | 55,977                           | 0.25%                        | 8,604                             |
| 43 (Preteen – Boy)                                        | 55,610                           | 0.25%                        | 7,128                             |
| 55 (The INDEXES)                                          | 55,088                           | 0.25%                        | 11,540                            |
| 49 (Trash Pen)                                            | 54,916                           | 0.25%                        | 11,921                            |
| 35 (Scat)                                                 | 50,550                           | 0.23%                        | 5,656                             |
| 67 (Français)                                             | 46,853                           | 0.21%                        | 3,097                             |
| 57 (Boys)                                                 | 44,783                           | 0.20%                        | 7,605                             |
| 28 (How to)                                               | 42,124                           | 0.19%                        | 8,416                             |
| 42 (Jailbait – Boy)                                       | 40,978                           | 0.19%                        | 5,601                             |
| 50 (Italiano)                                             | 34,581                           | 0.16%                        | 2,938                             |
| 21 (Playpen information and rules)                        | 32,051                           | 0.15%                        | 6,934                             |
| 27 (Feet)                                                 | 31,558                           | 0.14%                        | 3,696                             |
| 46 (Security & Technology discussion)                     | 30,848                           | 0.14%                        | 4,005                             |
| 18 (Boys SC/NN)                                           | 30,825                           | 0.14%                        | 3,441                             |
| 29 (Spanking)                                             | 29,653                           | 0.13%                        | 4,850                             |
| 54 (Netherlands)                                          | 21,628                           | 0.10%                        | 2,561                             |
| 36 (Fiction)                                              | 18,172                           | 0.08%                        | 4,200                             |
| 71 (Polski)                                               | 16,522                           | 0.08%                        | 2,052                             |
| 9 (Boys)                                                  | 12,583                           | 0.06%                        | 3,420                             |
| 20 (Boys SC/NN)                                           | 11,827                           | 0.05%                        | 2,102                             |
| 39 (Administration)                                       | 1,784                            | 0.01%                        | 15                                |
| 44 (PP members Torchat information exchange. (read only)) | 1,561                            | 0.01%                        | 402                               |
| 73 (Pre-Release)                                          | 465                              | 0.00%                        | 9                                 |
| 68 (Girls)                                                | 434                              | 0.00%                        | 11                                |
| 60 (Tools, Guides, and Discussion)                        | 393                              | 0.00%                        | 8                                 |
| 66 (Discussion and Rules)                                 | 75                               | 0.00%                        | 9                                 |
| 72 (Applications)                                         | 71                               | 0.00%                        | 12                                |

| Sub-Forum | Total number of<br>logged clicks | Logged clicks:<br>% of total | Total number of<br>unique members |
|-----------|----------------------------------|------------------------------|-----------------------------------|
| Total     | 21,967,663                       | 100.00%                      |                                   |

\* Some sub-forums had identical titles. As these sub-forums are located on different environments of the site and as they have their own content, they have their own ID number and they are considered different sub-forums in this table.

Researchers further analyzed which sub-forums were visited frequently in combination with each other. To do so, the number of clicks in each sub-forum for each member was calculated. Activities within sub-forums dedicated to various “fetishes” (bondage, chubby, feet, panties-nylons-spandex, peeing, scat, spanking, voyeur, and zoo) were compared with the main categories of “boy-lover” and “girl-lover” environments. Results from these combined sub-forum visits indicate that the majority of 80,111 members (82.4% of the total of members) were mostly active in girl-environments. Moreover, among a smaller number of members that were most active in the boy-environments (2,596 members, 2.7% of the total of members), approximately half (50.2%; or 1,303 members) also frequently visited girl-lover environments. And from the small minority of members who were most active in the fetish-environments (2,283 members, or 2.4% of the total of members), the majority also frequently visited girl-environments. Finally, there were a total of fifteen members active in the administration subforum, six of whom were most active in this particular sub-forum. Apart from their activity in this administrative environment, these members were found to visit the girl-environments most frequently. Four of them were most active within the hardcore environments, and two were most active within the softcore environments of the hidden service.

#### 5.3.2.2 Members’ downloading behavior

A final analysis calculated how frequently certain links containing CSE material files for download were accessed by unique members. Within the two-week timeframe analyzed, a total of 7,444,550 unique downloads were attempted among the 97,178 members. This equated to an average of 77 download attempts per member over a two-week period, or just under five download attempts per member per day. Only 6,235 members did not make any download attempt (6.4%).

Further examination of those members who made at least one download attempt (90,943 members), found that on average, these members were active on the website for approximately 3.5 days. Consequently, the 33,439 members who engaged in activity that was above the mean (four days or more), were further explored. Analysis

revealed that only 41 of these 33,439 members did not make any download attempt. Taken together, this means that of the approximately 33,452 members who were active on the website for more than four days, nearly all (99.9%) made at least one download attempt.

## 5.4 Discussion

The results from an overall descriptive analysis of the first dataset examining the “average” member on a CSE TOR hidden service suggest variation among members. Some members were active for only a short period of time, whereas others logged many hours of forum activity over a longer period of time. This result supports the notion of the existence of a relatively small group of keyplayer forum members (Fonhof et al., 2018), who play an important role in delivering content and moderation, and who are important for the hidden service’s existence and survival. Furthermore, the results from the analysis of the first login time on the hidden service demonstrate that the number of members that register during the very early days of the site’s existence is limited and that the number of registered members increased quickly from the beginning of September 2014 onwards. This implies that those members that registered in the first week the hidden service became public are potentially interesting and valuable targets for law enforcement. Their familiarity with the new hidden service could indicate that they have relevant ties to the broader CSE network, and that they may fulfill a key role in the site’s development.

Moreover, it is noteworthy that only a small percentage (3.4%) of members were verbally active on the hidden service. This is consistent with previous literature on lurking, which emphasizes that lurking is very normal internet behavior that constitutes a significant proportion of approximately 90% of all members active on the platforms (Gong et al., 2015; Mousavi et al., 2017; Nonnecke & Preece, 2000; Tagarelli & Interdonato, 2013). The fact that the percentage of lurkers is even higher in the current datasets is not surprising, as CSE hidden services are dedicated to taboo and illegal content/topics, about which members may be reluctant to speak about openly.

From the analysis of dataset 2 (the narrower two-week timeframe), it became evident that those members who were not verbally active, were still actively engaged with the website’s content and purpose, clicking and navigating through the various forums and sub-forums and (attempting to) download CSE material. Overall, 93.6% of forum members attempted to download illegal content. Of those members who were active on the site for at least four days, nearly all (99.9%) attempted to download CSE material. These results stress the need to emphasize that although the 96.6% of lurkers

represents the vast majority of forum members and may not be visibly or communicatively active, they are still engaged with the site's content and thus majorly impact on the CSE community. This study demonstrates the value of having had access to a specific and very detailed dataset of forum movements, comprising click data that highlights the hidden behavior of non-communicating members that would otherwise remain unknown.

Although the verbally active members may have the greatest public visibility on the site and the greatest potential of becoming a keyplayer, the potential risk of those members that are not verbally active should not be underestimated. Previous research on Darkweb CSE hidden services clarified that lurkers on one platform may actually be active participators on other locations. In the case of Darkweb CSE hidden services, members may use one platform/site for downloading solely and another platform/site to communicate with fellow members (Van der Bruggen & Blokland, 2021). Lurkers, once thought to simply be passive observers, are now understood to be more engaged and still have important ties with influential fellow members or with the larger network (Cranefield et al., 2015; Tagarelli & Interdonato, 2013). Moreover, law enforcement experience combined with findings from the current study and previous research also demonstrates that lurkers are still individuals that identify with the forum's predicated interests and experience a sense of belongingness to that community (Lutz & Hoffmann, 2017; Mousavi et al., 2017). Additionally, when one considers that 93.6% of members (attempt to) download illegal CSE material, it can be concluded that members intend to consume material related to those topics that interest them (Gong et al., 2015). Just like with any other member engaged on the site, the active pursuit and consumption of CSE material may affect attitudes and future behavior, which means that lurkers may also be a risk to children in the physical world. Therefore, the authors conclude that "being active" is a comprehensive and broad concept that includes unseen behavior, and illicit activities can be conducted without an obligation of verbal communication.

Additionally important, the results of this study imply that attempts to download illegal content is the main reason for the majority of members to visit the CSE hidden service. It is important to note that this finding applies to all members, despite their level of verbal activity on the site. Given the low number of members who were verbally active, combined with the broad downloading activities of all members, this particular CSE hidden service can be considered a download platform. This is also in line with the fact that the hidden service was an "open forum" (apart from having to register with a username and password, there were no further restrictions or activity requirements), with a low threshold to become and stay a member.

These findings have an important implication for law enforcement intervention.

Based on these findings, suspects testifying that they accidentally visited a CSE hidden service and unknowingly viewed/downloaded CSE material is not very plausible. The results of the current study imply that individuals active on Darkweb CSE hidden services, including the lurkers, purposefully and actively search for copious amounts of CSE material to view and download. Although a lack of resources contributes to law enforcement having to prioritize when dealing with large groups of suspects, the results of the current study infer that in addition to focusing on keyplayer members, there may also be value in detecting emotionally involved lurkers with high volumes of (attempted) downloads and movement activity (clicks) on the site.

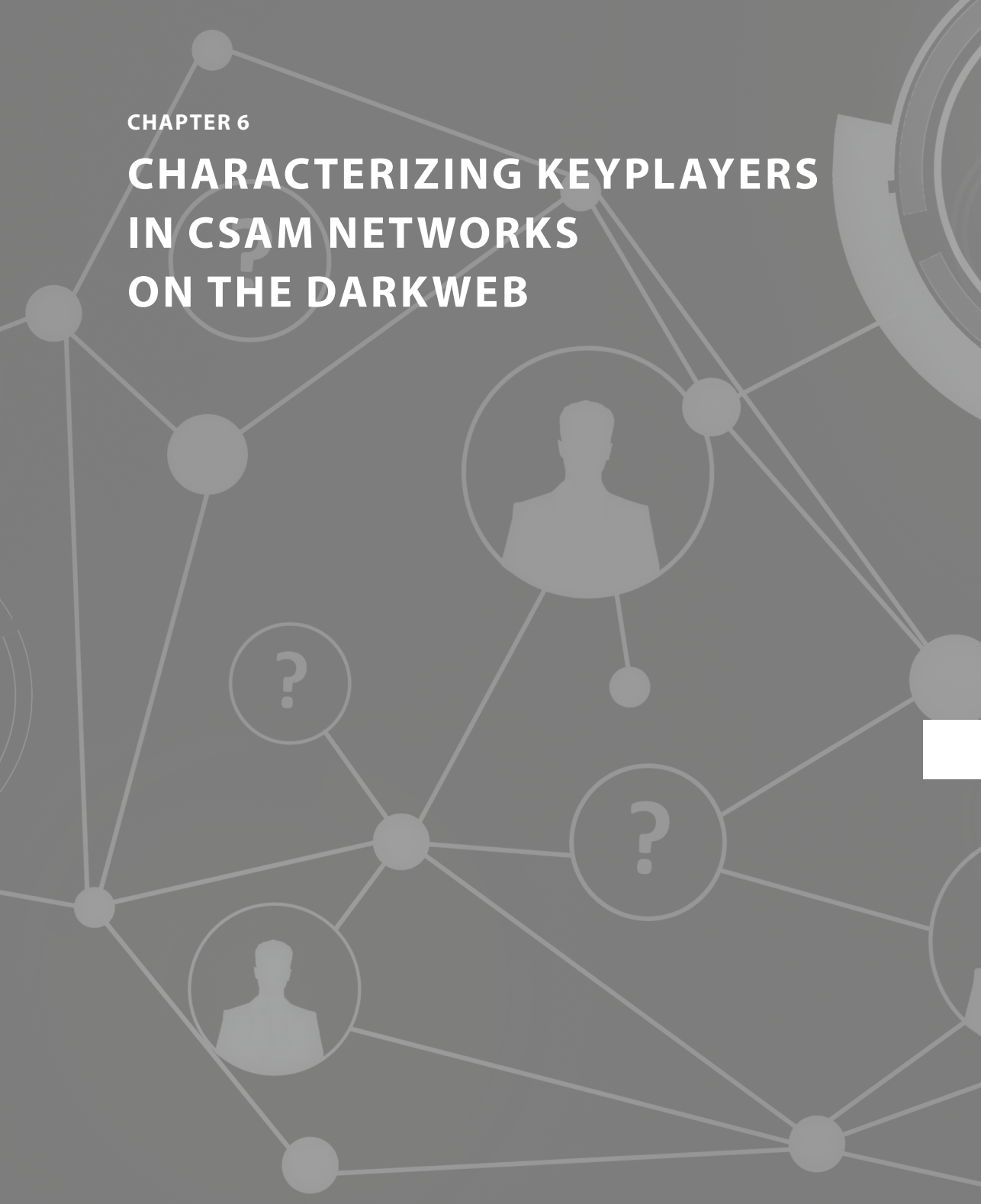
Finally, the hidden service analyzed in this study could be considered a “girl-lovers” site. The girl-related sub-forums were most popular, and based on their clicking and downloading behavior, most members (including the administrators) demonstrated a preference for girls. The group of members primarily interested in boys or other specific sexual interest such as fetishes, appear to be a small minority. This is not surprising, given Seto and Eke (2015) found that the majority of CSE offenders have a preference for girl content with their collections reflecting this preference. The group of offenders with exclusively boy material was very small, leading researchers to conclude that girl content was much more common. Consistent with this study, these findings can be partly explained by the members’ behavior and the logic behind the development of a site, that girl-environments will logically develop and expand (in terms of number of threads, potential material and links etc.) and consequently cause a greater volume of behavior flow. However, law enforcement experience indicates that there are separate and dedicated forums for “boy-lovers” or sexual fetishes. An interesting direction for future research would be to establish patterns in behavior flow and material downloaded across other Darkweb CSE hidden services, and potentially even to innovatively relate this to the specialization/versatility debate (Mazerolle & McPhedran, 2019).

The current study acknowledges a few limitations. Most importantly, only one CSE hidden service was analyzed during a limited timeframe, which affects the generalizability of the results. It is suggested that future research should compare the current results with CSE hidden services with a different focus, management style and levels of restriction. Moreover, the current study was not able to assess the content of attempted downloads, meaning that clicking on a link did not necessarily mean that the source file was ultimately accessed (the link could potentially be inaccessible, faulty or broken). Moreover, one cannot assume every link was associated with CSE material. However, this predicated hidden service was dedicated to and promoted the exchange of CSE material and the content uploaded to the site was moderated by the administrators. Furthermore, FBI special agents downloaded and reviewed over one million

files from this hidden service during their investigation and concluded that nearly all of the depicted files contained illegal CSE material (Department of Justice, 2019). The authors were, thus, fairly certain that an attempted download indeed concerned an illegal act.

Despite these limitations, the current study has value in informing operational practice, foremost because it focused on a platform (a Darkweb CSE hidden service) that attracted greater attention among CSE offenders at the time. It is important that research stays up to date with the (technical) developments of the crime field under study. Moreover, the fact that the current study had access to a unique dataset including all member clicks on the website, led to the conclusion that the verbally inactive members are no less important members within the hidden service community. Lurkers may be active downloaders, who may have evidence of these downloading activities on their computers. Moreover, they may even be contact offenders, or producers of CSE material in their physical life. The results of this study suggest that law enforcement should also focus on lurker members. Additionally, these results can inform forensic teams on what to look for during a search warrant. Moreover, the results of the current study may help prosecutors in explaining in court that despite no verbal activity, the chances are great that a suspect had a more active role in maintaining the CSE community by clicking through the site and attempting to download illegal material. With the results of the current study, the authors hope law enforcement investigators and prosecutors will be able to assess and compare the behavior of individual suspects, using a more accurate “general profile” of members. For example, prosecutors could exemplify that a certain suspect deviates from the general profile regarding the number of visits, clicks, and downloads on a hidden service. Building on this research direction, eventually a more complete insight into the anonymous online CSE offender population will be gained.



The background of the page features a complex network diagram. It consists of numerous circular nodes of varying sizes, interconnected by thin, light-colored lines. Some of these nodes are replaced by larger circular icons containing a silhouette of a person or a question mark. The overall aesthetic is technical and digital, with a dark gray background.

## CHAPTER 6

# CHARACTERIZING KEYPLAYERS IN CSAM NETWORKS ON THE DARKWEB

***This chapter has been published as:***

Fonhof, A., Van der Bruggen, M., & Takes, F. (2018). Characterizing keyplayers in child exploitation networks on the dark net. *Complex Networks*, 813, 412-423.

[https://doi.org/10.1007/978-3-030-05414-4\\_33](https://doi.org/10.1007/978-3-030-05414-4_33)

## Abstract

This paper studies online child exploitation networks in which users communicate about illegal child pornography material. Law enforcement agencies are extremely interested in better understanding these networks and their keyplayers. We utilize unique real-world network datasets collected from two different online discussion forums on the dark net. Our study of the network structure underlying these forums results in three contributions. First, we propose an approach to identify keyplayers using various centrality measures, allowing us to automatically rank users. Experiments show that our method closely resembles a network-agnostic ranking of users created by domain experts. Second, network metrics are able to characterize a large portion of the users, allowing us to distinguish between regular users, managers and technical moderators. Finally, analyzing the structural properties and distributions of these networks in both the one-mode and two-mode perspective reveals various interesting network-driven insights, such as anti-lurker and anti-law enforcement policies and new user application guidelines. In addition, we found that active users form an elite that participate in more specialized discussions.

## 6.1 Introduction

Child pornography can be defined as any visual depiction of sexually explicit conduct involving a minor. It has serious damaging effects on the victims and can be considered one of the key social security problems, especially in today's digital society. With the emergence of the dark net (a part of the internet that requires specific software or authorization, see: Egan, 2018) the access to child pornography has been made more secure and anonymous, resulting in growing numbers of users. These factors have made it increasingly valuable to have the right methods and techniques that help agencies to prioritize their law enforcement activities.

In this paper we study data originating from online discussion forums on the dark net. Offenders use these forums to distribute and communicate about illegal child abuse material (Van der Bruggen & Blokland, 2018). Such platforms are often moderated and organized in a professional manner, serving hundreds of thousands of users. To efficiently coordinate law enforcement activities, it is important to target keyplayers that are vital to the existence of these forums, such as administrators, technical moderators and abusers. In this paper we will explore this data as a network and at-

tempt to automatically identify these keyplayers and their role using various network science methods and techniques (Barabási, 2016).

A forum consists of topics and allows multiple users to respond on a certain topic by placing a message, also called a post. This activity can be modelled using a two-mode *topic-to-user* network. To also observe the direct social relationships emerging on these forums, we also project our network to a *user-to-user* network. This allows a number of methods to better understand the network structure to be applied. However, a lot of information in the two-mode network is lost after projection, e.g. how many topics two users responded to or how big a certain topic is that connects two users. Projection can also lead to one-mode network properties that are a result of the projection process rather than the underlying social structure, for example a topic that is linked to many users, which we call a ‘big linker’. In the considered child exploitation networks, if two users are linked because they commented on a big generic ‘Introduce yourself’-topic, this link is of less significance than if they commented on a specific abuse-related topic. Therefore, we explore different types of projection algorithms in an attempt to select the method which best recreates the forum’s underlying social structure.

This paper provides three contributions. First, we study the social structure of the child exploitation networks in an attempt to understand their functioning and governance structure. Second, we analyze the effect of various projection methods on the structure of this network, enabling the third contribution: automated identification of keyplayers and the characterization of user roles.

The rest of this paper is structured as follows. In Section 6.2 we formulate the notions and algorithms that are used in this paper. Related research is discussed in Section 6.3. We describe the data in Section 6.4. Then the proposed approaches are outlined in Section 6.5. Next, experiments are performed in Section 6.6. Finally, conclusions are drawn and future work is suggested in Section 6.7.

## 6.2 Preliminaries

In this section we discuss the terminology and network metrics used in this paper, adapting the notation of two-mode and one-mode networks by Latapy et al. (2008). Note that there is some minor overlap in notation and symbols for two-mode and one-mode networks. In the remainder of the paper, whenever the context requires so, we will explicitly state in which type of network we are considering the metric.

### 6.2.1 Two-mode networks

A two-mode (or bipartite) network is made up of two different sets of vertices in which ties exist only between vertices belonging to different sets. The two sets of vertices are users and topics and a tie is a comment that a user posts on a topic. A distinction is often made between the two vertex sets based on which set is considered more responsible for tie creation (called the primary or top vertex set) than the other (secondary or bottom vertex set). We denote a two-mode graph as  $G = (T, \perp, E)$  where  $T$  is the set of top vertices,  $\perp$  is the set of bottom vertices and  $E \subseteq T \times \perp$  is the set of undirected edges. In the considered child exploitation networks the topics are the top vertex set, the users are the bottom vertex set, and links denote a user commenting on a certain topic. We will denote the number of top and bottom nodes as  $n_T = |T|$  and  $n_\perp = |\perp|$ , respectively and the total number of nodes is denoted  $n = n_T + n_\perp$ . We denote the number of edges as  $m = |E|$ . We can then define the top and bottom average degree as  $k_T = (m/n_T)$  and  $k_\perp = (m/n_\perp)$ , respectively. The total average degree is defined as  $\langle k \rangle = (2m/(n_T + n_\perp))$ .

### 6.2.2 One-mode networks

After projection (which we discuss in Section 6.5.1) we have a one-mode social network  $G = (V, E)$  in which users (so,  $V = \perp$ ) are connected by a set of social interaction edges  $E$ . An edge denotes that two users replied to the same topic, possibly with an edge weight, dependent on the employed projection method (see Section 6.5.1). We again denote the number of nodes as  $n = |V|$  and the edge count as  $m = |E|$ , and use  $k(v)$  for the degree of a node  $v$ . The average degree  $\langle k \rangle = \frac{1}{n} \sum_{v \in V} k(v)$  is computed by averaging the degree over all nodes. The distance  $d(u, v)$  is the length of a shortest path between two nodes  $u$  and  $v$ . The average path length over all node pairs is denoted by  $\langle d \rangle$ .

The diameter  $d_{max}$  is the maximum distance over all node pairs. The degree assortativity coefficient  $r$  describes how nodes are preferentially connected based on their degree, and is defined as:

$$r = \frac{\sum_i e_{ii} - \sum_i a_i b_i}{1 - \sum_i a_i b_i}$$

Here,  $a_i = \sum_j e_{ij}$  and  $b_j = \sum_i e_{ij}$ , where  $e_{ij}$  is the fraction of edges from a node with degree  $i$  to a vertex with degree  $j$ . When  $r > 0$  the network is said to be assortative and when  $r < 0$  it is disassortative. The average neighbor degree is the average degree of a node's neighbors. The weighted degree of a node  $v$  is the sum of edge weights of nodes adjacent to  $v$ . The average weighted degree connectivity is the average nearest neighbor weighted degree of nodes with weighted degree  $k$ . For further details of these metrics, the reader is referred to Barabási (2016).

## 6.3 Related work

Below we briefly discuss related work on criminal networks, child exploitation networks and methods to identify keyplayers.

In a recent study, Van der Bruggen and Blokland (2021) discuss child pornography on the internet, arguing that child exploitation networks on the dark net could be classified as criminal organizations. In Duijn (2016), the use of network analysis for detecting and disrupting criminal networks was investigated, yet, child exploitation networks remained beyond the scope. Westlake et al. (2011) studied child exploitation networks, in particular as a connection between websites. They identified the most important website to target for law enforcement based on a metric called network capital.

Latapy et al. (2008) introduce a set of metrics to capture properties of interest in two-mode networks. They provide an alternative to the projection approach, emphasizing that (weighted) projection approaches also produce compelling insight and that the two approaches should be used in an interdependent manner to thoroughly understand the properties of two-mode networks. In this paper, we will evaluate these claims on our two-mode child exploitation network data.

Identifying keyplayers is typically done using centrality measures. More detailed methods for finding keyplayers in social networks, such as those suggested by Borgatti (2006) are aimed at specific tasks, such as optimally transmitting a message through the network or fragmentation of the network by the removal of certain users. However in this paper, we aim to rank the entire set of network users.

## 6.4 Data

We use two different network datasets, referred to anonymously as dataset A and dataset B due to it being law enforcement sensitive data. The data originates from two distinct child exploitation forums on the dark net that have been taken down by law enforcement and are no longer in operation. Below, we discuss the two forums as well as the metadata added by domain experts.

### 6.4.1 Forum data

Dataset A consists of 14,659 users and spans a 4 year time period from 2010 to 2014. In order to get access to this forum, users had to provide abusive content that had to be verified by admins. It featured a tiered system, meaning that users were given access to special topics if they presented more unique or self-produced material. This allowed users to gain prestige in the network by actively contributing.

Dataset B has 21,257 users, spans 2 years and was in operation from 2015 to 2017. This forum had a standard approach to user registration, giving users access to almost all topics, apart from a few protected topics for producers and administrators.

The remainder of this paper explores these two-mode networks and their properties. For both datasets, users that did not comment on any topic were excluded, which means that the actual number of members may have been much higher than the number of users included in our study. Furthermore, only unique identifiers for users and topics are studied; no textual or image data was included in this study. Further statistics are provided in Section 6.6.1.

#### 6.4.2 Domain-specific node metadata

Researchers at the Dutch National Police performed the so-called Program Identifying Main Targets (PIM) analysis, partially based on Nolker and Zhou (2005). It uses forum conversation analysis, language analysis and TF/IDF metrics of conversation importance to determine membership roles as well as a ranking of keyplayers.

##### 6.4.2.1 PIM membership roles.

Users were divided into four groups (each with their own percentage of occurrence in dataset A and B):

- **Managers** (0.49% of A, 3.52% of B) are responsible for organizing the forum, recruiting and welcoming new members and enforcing rules.
- **Abusers** (0.59% of A, 4.1% of B) communicate extensively about child abuse and share experiences and fantasies with the community, encourage others to commit criminal activities and may also produce material themselves.
- **Technical users** (0.4% of A, 3.14% of B) focus on developing and sharing anonymity software and providing technical support to other users.
- **Embedded users** (98.3% of A, 89.24% of B) are users that do not fall into any of the first three groups.

##### 6.4.2.2 PIM ranking

A numeric metric was devised by domain experts to assign a value to each user determining its importance. It combines the aforementioned forum conversation analysis and TF/IDF metrics of conversation importance. In addition, users who used particular words identified by domain experts to be characteristic for important users, received a higher metric value. In the PIM ranking, users are ordered by this particular metric value. For details, see Nolker & Zhou (2005).

## 6.5 Approach

First, Section 6.5.1 discusses the different types of projection methods. Then, Section 6.5.2 explains how we propose to identify and characterize key users.

### 6.5.1 Determining the right projection method

Here, we build on the definitions in Section 6.2, looking in detail at how the projection from a two-mode to a one-mode network assigns weights to the nodes. The  $\top$ -projection of graph  $G$  is denoted  $G_{\top} = (\top, E_{\top})$ . Two nodes of  $\top$  are linked if they share at least one neighbour in the two-mode network, so  $E_{\top} = \{(u, v), \exists x \in \top: (u, x) \in E \text{ and } (v, x) \in E\}$ . The  $\perp$ -projection is defined analogously. To uncover the underlying social structure of the forums, in this paper we look at the *user-to-user* network and are therefore only interested in the  $\perp$ -projection. We will study three projection methods:

- **Unweighted projection** creates an unweighted undirected network of users that commented on the same topic at least once. As mentioned in Section 6.1, here the number of topics that two users commented on is lost.
- **Weighted projection** assigns a weight  $w_{u,v} = |N(u) \cap N(v)|$  to each edge  $(u, v)$  in the projected network denoting the number of common topics  $u$  and  $v$  commented on, where  $N(v)$  is the set of neighbors of  $v$  in the two-mode network. This retains information on the number of topics.
- **Newman's collaboration model** (Newman, 2001) assigns a weight as follows:

$$w_{u,v} = \sum_x \frac{\delta_u^x \delta_v^x}{k(x) - 1}$$

Here,  $\delta_u^x$  is 1 if  $(u, x) \in E$  in the two-mode network, and 0 otherwise. Also,  $u$  and  $v$  belong to the  $\perp$  node set and  $x$  belongs to the  $\top$  node set. The value of  $k(x)$  is the degree of  $x$  in the two-mode network and  $\delta_u^x$  is 1 if node  $u$  is linked to node  $x$  in the two-mode network, and 0 otherwise.

For the remainder of the paper, for computing distances, we inverse the weights (so,  $w_{u,v} = \frac{1}{w_{u,v}}$ ), so a lower weight indicates more relatedness of users.

### 6.5.2 Key user characterization

Users that play a significant role in a network supply human capital, which consists of services that are of importance to the survival of the forum network (Duijn, 2016). For example moderating topics, recruiting new users, distributing resources or helping

users with technical questions. To identify these users we will focus on largest connected component (see Section 6.2.2) of the one-mode *user-to-user* network, considering the following metrics:

- **Degree centrality**  $C_D(v)$ : the fraction of nodes that user  $v$  is connected to, defined as  $C_D(v) = \frac{1}{n-1} k(v)$ .
- **Closeness centrality**  $C_C(v)$ : this metric computes the distance of node  $v$  to each other node in the network. To deal with multiple connected components, we use the highly similar harmonic centrality, formally defined as  $C_C(v) = \frac{1}{\sum_u d(u,v)}$ .
- **Eigenvector centrality**  $C_{EV}(v)$ : determines the centrality of a node based on how central, or well-connected, its neighbors are, see Bonacich (1987) for details.
- **PageRank**  $C_{PR}(v)$ : is a metric that ranks nodes based on the likelihood that a random surfer in the network will arrive at that node, see Brin and Page (1998) for details.
- **Betweenness centrality**  $C_B(v)$ : this measure computes the number of shortest paths that run through a node  $v$ . With  $\sigma_{st}$  the number of shortest paths from  $s$  to  $t$  and  $\sigma_{st}(v)$  the number of shortest paths from  $s$  to  $t$  that pass through vertex  $v$  it is defined as  $C_B(v) = \sum_{\substack{s \neq v \neq t \in V \\ s \neq t}} \frac{\sigma_{st}(v)}{\sigma_{st}}$ .

To rank users, we propose to sort users by either one of the centrality metrics. To identify the role of a user, we compare the centrality measures between the different roles (as defined in Section 6.4.2). Through this approach we furthermore gain insight in the applicability of these metrics in understanding user roles automatically.

## 6.6 Results

We explore the characteristics of the two-mode networks in Section 6.6.1. Then we compare the different projection methods in Section 6.6.2. Section 6.6.3 builds upon the projected network, investigating our methods of ranking keyplayers. Finally, Section 6.6.4 analyzes the centrality measurements of different user roles.

### 6.6.1 Network characteristics

Table 6.1 shows basic statistics about the topology of the two-mode networks. Interesting to note is the relatively large number of top nodes ( $n_{\top}$ ) and the high average degree for the bottom nodes ( $k_{\perp}$ ) in dataset A.

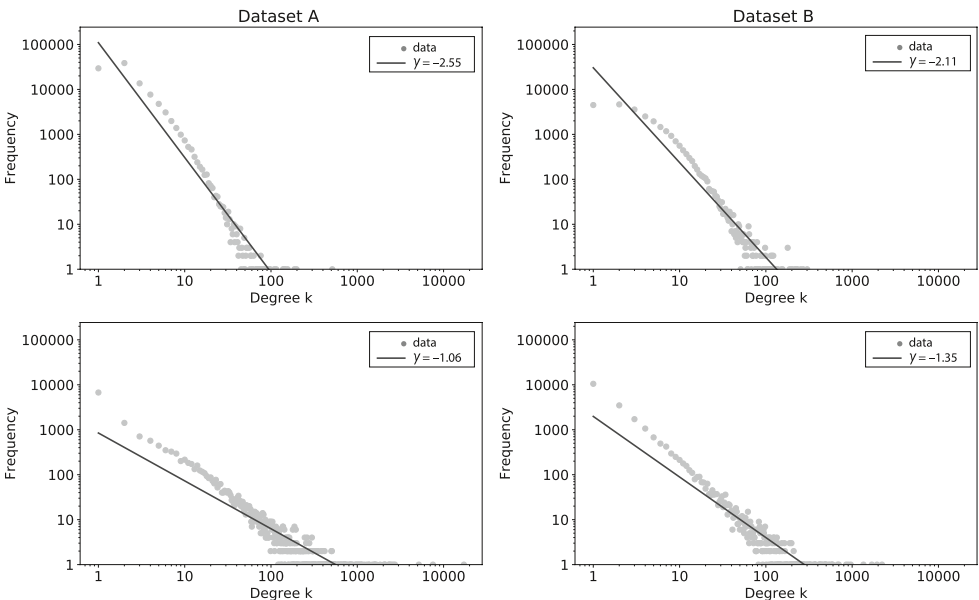
**Table 6.1 Two-mode network statistics of the two datasets**

|                                    | Dataset A | Dataset B |
|------------------------------------|-----------|-----------|
| Nodes $n$                          | 119,742   | 46,313    |
| Topics $n_T$                       | 105,083   | 25,056    |
| Users $n_U$                        | 14,659    | 21,257    |
| Posts $m$                          | 309,716   | 145,086   |
| Average degree $\langle k \rangle$ | 5.2       | 6.3       |
| Average topic degree $k_T$         | 3.0       | 5.8       |
| Average user degree $k_U$          | 21.1      | 6.8       |

6.6.1.1 Degree distributions

The above mentioned difference in average degree can be understood by looking at the degree distribution, shown in Figure 6.1. In real-world data, these distributions follow a power law with exponent  $\gamma$  (Barabási, 2016). We observe that that the top nodes (topics) of dataset A have a higher value of  $\gamma$  than in dataset B, which may indicate that there is more emphasis on smaller topics in dataset A. For the bottom nodes (users) we see the opposite pattern; in dataset A,  $\gamma$  is lower than in dataset B. This indicates that a few users in dataset A comment on almost all topics, which explains the relatively high average value of  $k_U = 21.1$  in dataset A.

**Figure 6.1 Degree distribution of topics (first row) and users (bottom row)**

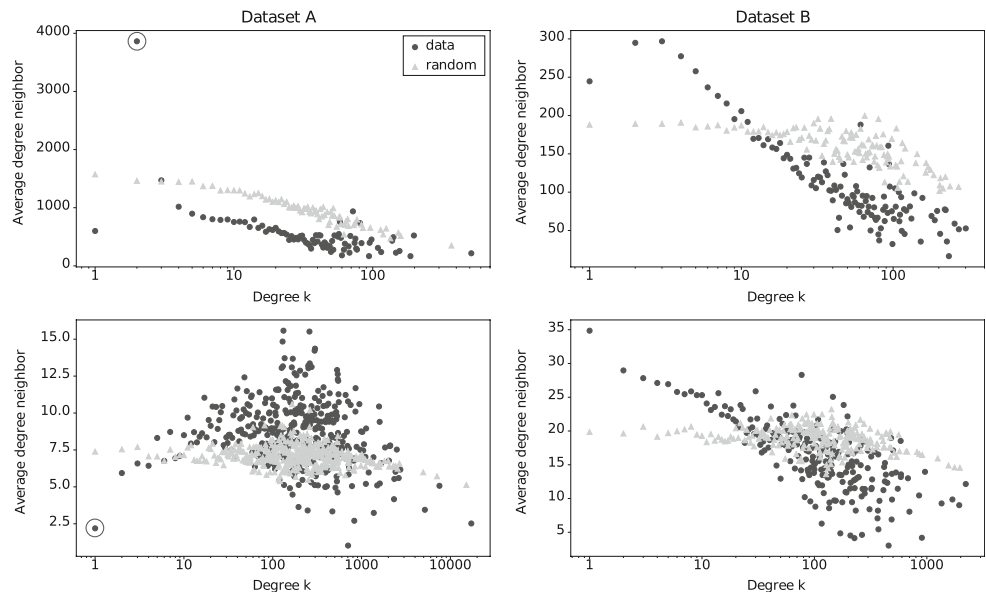


#### 6.6.1.2 Average degree connectivity

Figure 6.2 shows the average degree connectivity (see Section 6.2) for both topics and users. For reference we also plot this value for a random two-mode network with the same degree sequence, generated using the configuration model. The figure highlights various interesting phenomena.

First, the top nodes in dataset B display a negative trend, suggesting that larger topics are commented on by users that are on average less active. However, as shown in Figure 6.2, the bottom nodes (users) do not show this negative correlation. In fact, the most active users comment on topics with relatively few comments. Second, in dataset A topics with 2 comments are on average commented on by users with an average degree of almost 4,000 (highlighted top left node). According to the degree distribution shown in Figure 6.1 there are only a handful of users with a degree larger than 4,000. It turns out that this is the result of the application process of the forum represented by dataset A, where new users had to make an application to gain access, which had to be approved by an administrator (with the high average degree). The bottom left plot of Figure 6.2, showing the average degree connectivity of users, highlights a similar phenomenon occurring at degree  $k = 1$  with an average degree connectivity of 2. This represents users who commented once and did so on a topic with only 2 comments; again the aforementioned application topic. This can essentially be seen as an anti-lurker or anti-law enforcement policy; access to the forum is restricted to those who do not provide content. The bottom row of the figure shows that in dataset A there are relatively high post counts for high degree users, indicating that users keep participating and contributing content over time. Altogether, this demonstrates the existence of the tiered system in dataset A, mentioned in Section 6.4, where users providing content were given access to more specialized topics. This pattern was not found in dataset B, which indeed also did not have this policy.

**Figure 6.2** Average degree degree connectivity of topics (first row) and users (bottom row)



### 6.6.2 Comparing projections

To assess which projection method works best, Table 6.2 shows the degree assortativity coefficient  $r$  for each of the discussed projection methods. It is highest in both datasets for the weighted projection and Newman collaboration projection. In these two projections, the weighted degree of a node is now scaled by the strength of its relationships. This could imply that using weights better encompasses the phenomenon that users connect with users who are also well connected.

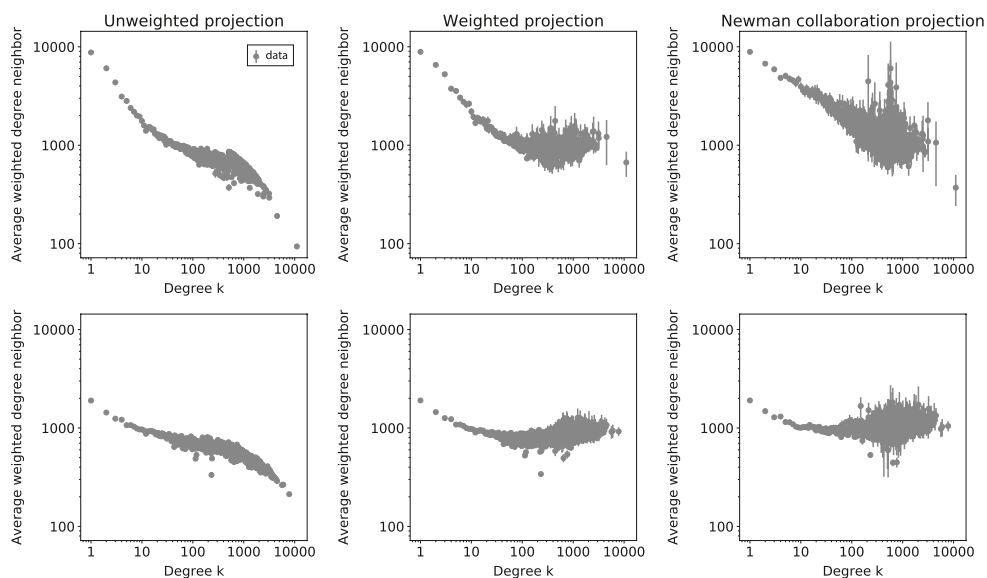
**Table 6.2** Degree assortativity coefficient of the projected graphs

|     | Dataset A  |          |        | Dataset B  |          |        |
|-----|------------|----------|--------|------------|----------|--------|
|     | Unweighted | Weighted | Newman | Unweighted | Weighted | Newman |
| $r$ | -0.137     | -0.123   | -0.038 | -0.109     | -0.076   | -0.049 |

We further examine this by plotting the average weighted degree connectivity (see Figure 6.3). The leftmost plot of unweighted projection, shows for both datasets a weak negative trend, which may imply that the more users you are connected with the less well connected your neighbors are. However, when we add weights to the edges

this effect disappears. This explains the increasing  $r$  in Table 6.2; it puts additional emphasis on a user that is talking to other important users. Through discussions with domain experts we validated that well connected users are indeed more inclined to chat with other well connected users. In other words: the more important a member is for the community, the more well-connected he is and the more likely to communicate with other well connected users. This can be seen as the existence of an elite of active users. All in all, these experiments suggest that adding weights (either with weighted projection or Newman projection) gives a more accurate representation of the underlying social structure of users.

**Figure 6.3 Average weighted degree connectivity of the three projected graphs. The first row shows dataset A and the second row shows dataset B**



### 6.6.3 Identifying keyplayers

The ranking of users based on centrality metrics is influenced by the type of projection used. Therefore, for each of the five centrality metrics in Section 6.5.2 we compute for each of the three projection methods in Section 6.5.1 how well it reproduces the aforementioned PIM ranking (see Section 6.4.2). To do so, we compute the Spearman rank-order correlation coefficient (Ziegel, 2001) between the PIM ranking and the considered centrality measure. A value close to 1 (or -1 for a negative correlation) indicates more agreement on the ordering, whereas a value of 0 means that the rankings are unrelated.

Table 6.3 shows the rank-order correlation coefficients. For both datasets, the weighted projection method outperforms the other two types of projection in recreating the PIM ranking. This is a second piece of evidence suggesting that weights need to be incorporated in the projection step in order to capture important patterns in user interaction. In dataset A we see as much as a rank-order correlation of 0.79 when we use closeness centrality with a weighted projection. In dataset B we have a rank correlation 0.57 with PageRank and the weighted projection method. This shows how a global ranking based on centrality is able to accurately reproduce the PIM ranking generated by domain experts.

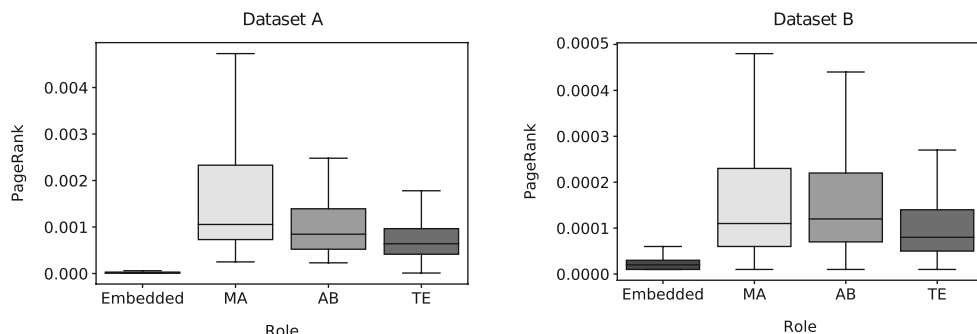
**Table 6.3 Spearman rank correlation between PIM ranking and centrality metrics**

|           | Unweighted |       |          |       |          | Weighted |       |          |       |          | Newman |       |      |       |      |
|-----------|------------|-------|----------|-------|----------|----------|-------|----------|-------|----------|--------|-------|------|-------|------|
|           | $C_B$      | $C_C$ | $C_{EV}$ | $C_D$ | $C_{PR}$ | $C_B$    | $C_C$ | $C_{EV}$ | $C_D$ | $C_{PR}$ | $C_B$  | $C_C$ | EV   | $C_D$ | PR   |
| Dataset A | 0.5        | 0.46  | 0.35     | 0.44  | 0.47     | 0.57     | 0.79  | 0.75     | 0.44  | 0.76     | 0.52   | 0.77  | 0.76 | 0.44  | 0.75 |
| Dataset B | 0.54       | 0.43  | 0.43     | 0.51  | 0.53     | 0.55     | 0.53  | 0.46     | 0.51  | 0.57     | 0.53   | 0.44  | 0.42 | 0.51  | 0.55 |

#### 6.6.4 User roles

The goal of user role identification is to find network-driven characteristics that help understand the position of particular groups of users. In the subsection above we found that PageRank had the highest rank-order correlation in dataset B, and the second highest in dataset A. Figure 6.4 shows the differences between the user roles (see Section 6.4.2), again based on PageRank. We observe that users with a special role (managers (MA), abusers (AB) and technical users (TE)) consistently have a more central position than embedded (regular) users. Furthermore, managers and abusers are in turn more central than technical users, which can be explained by the fact that these keyplayers are more individualistic and focus more on building applications, mainly talking with their peers. Managers on the other hand have to communicate with all users and are thus more central.

**Figure 6.4 Distribution of PageRank values with weighted projection for different user roles (see Section 6.4.2)**



## 6.7 Conclusion and future work

In this paper we studied two unique network datasets from online child exploitation forums, in which users comment on certain child abuse related topics. Through analyzing the degree distribution of the two-mode network we found that larger topics are commented on by relatively less active users, likely because these topics are more easily found and talk about a more easily accessible subject. Topics with few comments were commented on by relatively more active users, hinting at the existence of an elite of users contributing to more specialized discussions, containing keyplayers with roles important to the forum. The average degree connectivity of dataset A revealed the admission procedure of this forum, where users had to provide content in order to gain access to the forum. We also discovered that using a weighted form of projection to obtain the one-mode network is crucial for obtaining the network's underlying social structure of the user-to-user network. Using weighted projection and closeness centrality we were able to obtain a high (up to 79% for dataset A) rank-order correlation coefficient with a ranking of users generated by domain experts. This demonstrates the power of network metrics in identifying keyplayers. Finally, we evaluated the different user roles, and found that it is possible to distinguish between regular users and keyplayers based on their centrality values. It furthermore revealed the more individualistic role of technical users dealing with the forum setup, encryption and maintenance. In general, the proposed network approach has a number of advantages over content-based analysis of dark net forum data, as it only requires the structure of the forum, and as such can deal with encrypted posts and forums in unknown foreign languages.

In future work, we want to investigate if we can devise a classification model to accurately determine the role of a given user, building upon the results of the analysis

and characterization of user roles through centrality. Furthermore, we want to investigate private messages sent on the forums in an attempt to understand the extent to which the observed social interaction in the projected networks captures direct social interaction in the network.





CHAPTER 7

# TRUST AND RELATIONSHIP DEVELOPMENT IN DARKWEB CSAM NETWORKS: A LITERATURE REVIEW FROM A PSYCHOLOGICAL AND CRIMINOLOGICAL PERSPECTIVE

***This chapter has been published as:***

Kloess, J., & Van der Bruggen, M. (2021). Trust and relationship development among users in Dark Web child sexual exploitation and abuse networks: A literature review from a psychological and criminological perspective. *Trauma, Violence & Abuse*. Advance online publication. <https://doi.org/10.1177/15248380211057274>

## Abstract

The increased potential and speed of the internet has changed the nature of sexual crimes against children. It enables individuals with a sexual interest in children to meet, interact, and engage in illegal activities. The literature review presented here aims to provide an overview of the current knowledge and understanding of trust and relationship development among users of online networks that are dedicated to the sexual exploitation and abuse of children. A systematic search using six databases was conducted to identify relevant literature from a psychological and a criminological perspective. Twenty-one studies met the inclusion criteria that centered around the key aspects of the literature review's research question, namely, (i) child sexual exploitation and abuse, (ii) Dark Web platforms, (iii) online forums and networks, and (iv) trust and relationship development. Our findings reveal that the engagement in interpersonal communication and interactions with like-minded others serves various functions, including validation, normalization, and support, as well as access to expert advice, information, and material. Dark Web networks are high-stake and risky environments, where users have to manage a continuous flow of threats, with information about others and their trustworthiness being limited. The establishment and maintenance of trust is of social and technical relevance, and users have to navigate a number of demands and commitments. Findings are discussed in relation to theoretical and practical implications, as well as directions for future research.

## 7.1 Introduction

Child sexual exploitation and abuse (CSEA) has existed long before the emergence of the internet; however, new opportunities for offending are afforded by the online environment and its Triple A Engine, namely, anonymity, accessibility, and affordability (Cooper, 1998). This makes the internet an attractive environment to seek out and pursue certain types of information and material, as well as engaging in various activities, while at the same time keeping one's identity and participation hidden. It also enables individuals to connect with a large number of users without the restrictions of geographical proximity, and existing social networks (Leukfeldt et al., 2017). While the Surface Web allows individuals to adopt online identities or personas that are difficult to verify, the Dark Web offers additional "protection" by facilitating "near-com-

plete anonymity” (Chiang, 2020) through its extra layers of encryption. More specifically, the Dark Web refers to a “part of the World Wide Web that can only be accessed using special software, such as The Onion Router (TOR), Freenet and I2P. It contains content that cannot be indexed by traditional search engines and provides anonymity for users and website operators” (National Crime Agency, 2019, p. 6).

The Dark Web is a space where users can find anything from illegal drugs to stolen identities, as well as child sexual exploitation material (CSEM), and has a reputation of catering to some of the most notorious interests and goods through various platforms, with users taking advantage of its privacy and obscurity (Ntrepid, 2019). As part of these online communities and markets, users share advice and information, as well as best practices and recommendations, often relating to privacy, security, and avoiding detection, which enables “newbies” to learn from those with substantial experience of operating on the Dark Web (Chiang, 2020).

For users who are interested in (i) trading and sharing CSEM for personal or commercial reasons, (ii) communicating with like-minded individuals who have a sexual interest in children, and (iii) maintaining and developing “online pedophilic networks” (Beech et al., 2008), the internet presents an ideal environment for pursuing and getting involved in these activities. Previously, individuals faced constant challenges and great personal risk when attempting to access material of this nature in the physical world. The internet now enables users to connect with like-minded individuals across the world to form communities that offer moral validation, social support, and instant access to a continuous flow of information and material (Westlake & Bouchard, 2016).

Until 2017, when an international law enforcement operation conducted by Taskforce Argos, a branch of the Queensland Police Service in Australia, highlighted the deployment of undercover police officers by law enforcement agencies in an attempt to proactively investigate sexual offenses against children, offending behavior that takes place on the Dark Web had received little attention. By the time law enforcement took one of the main forums dedicated to CSEA on the Dark Web offline, the site had attracted one million user registrations. According to The Guardian (2017), 3,000–4,000 individuals were active users, and around 100 of these regularly produced and shared CSEM with the community.<sup>1</sup>

In 2019, the National Crime Agency in the UK identified 181,000 individuals

<sup>1</sup> It is important to highlight, however, that some users may subscribe numerous times, inflating the overall number of registrations. In addition, the number of one million user registrations may also include bots and accounts created by law enforcement personnel. The article does not clearly state whether the one million user registrations refer to unique users. Furthermore, their reference to active users raises the question of what it constitutes – it may refer to a user who has communicated and interacted on the site, or someone who has regularly logged in. Again, this is not clear from the article.

who were members of organized crime groups and operated on some of the most problematic sites on the Dark Web that were dedicated to CSEA. It is of note that this number merely includes users who are known to be engaging in offending behavior and therefore represents a conservative estimate. The agency's National Strategic Assessment of Serious and Organised Crime (2019) revealed that there were nearly 2.9 million accounts registered on these sites worldwide, with 5% believed to be from individuals residing in the UK. More worryingly, the number of referrals of identified occurrences of online CSEA from industry to the agency has increased by 700% since 2012 (National Crime Agency, 2019). The agency argues that the anonymity afforded by the Dark Web continues to attract individuals who engage in serious and organized crime, with TOR being the main access point to services on the Dark Web. Furthermore, an ongoing growth in the volume of criminal trade notifications on TOR-based platforms has been noted, with CSEA online remaining a high-volume offense, and recorded instances of offending behavior increasing across the UK (National Crime Agency, 2019), including the amount of CSEM that is being distributed (Europol, 2019).

Among the conclusions derived from the threat assessment undertaken by Europol (2019) was that the Dark Web is a key enabler for the trading in a wide range of criminal products and services. Although government and law enforcement agencies, as well as industry, have been publishing relevant figures and rates that give an indication of the ever-increasing problem they are facing in terms of tackling the use of the Dark Web for illegal activities, relatively little is known about the nature and role of CSEA forums on the Dark Web that are frequented by a large number of users (Finklea, 2017). In fact, what characterizes these forums is the enormous difficulty in accessing them for research purposes due to their illegal nature, and studies that specifically examine them (and other types of Dark Web forums) are therefore scarce.

Most studies that have been conducted from a psychological perspective have predominantly examined offenders' characteristics and demographics, their motivations, and psychological variables, as well as conviction and reoffending rates, with a particular focus on individuals who view, download, distribute, or produce CSEM, and therefore access relevant platforms for these purposes, on the Surface Web. Some may be primarily motivated to access and download CSEM for the purpose of sexual stimulation, arousal, and gratification, whereas others may be driven to complete series of images and build a collection (Quayle & Taylor, 2002; Rimer, 2019). Again, others may be motivated by the financial gain associated with dealing with this type of material.

The few studies that have looked at the nature and role of online communities and networks, geared toward individuals with a sexual interest in children, have

found that their organizational structures are similar to pedophile rings and other criminal networks in the physical world, and that they provide users with a space that serves the function of social and peer support, validation, and access to expertise. More specifically, the online environment provides users with opportunities to access a wide range of information and resources, as well as corresponding and interacting with like-minded individuals. Groups of individuals form communities online which act to validate users' attitudes and beliefs, as well as their sexual interests, preferences and behaviors. Something that keeps them attractive, and suggests popularity, is the increasing membership, and the fact that these platforms are uncensored and peer-moderated spaces, enabling users to interact freely without constraints and sanctions. These groups or communities thereby take on the role of a support mechanism or system for individuals who have a sexual interest in children, which is absent in their lives in the physical world (Holt et al., 2010; Martellozzo, 2015).

Studies from a criminological perspective have emerged that specifically explore group dynamics, such as the development of trust, in cybercriminal networks on the Dark Web, including those geared toward hackers and marketplaces where illegal goods (e.g. drugs and weapons) are exchanged. A small number of these studies also focus, in part, on networks that are dedicated to CSEA. The question arises as to how cooperation and trust (defined as a mechanism to “cope with risk and uncertainty in interactions with others”; (Von Lampe & Johansen, 2004, p. 103) between co-offenders is established under conditions where users do not know each other's true identity, where no regulatory body is present to enforce rules, and where trust may, therefore, be easily betrayed (Lusthaus, 2012). Here, criminological studies have reported similar findings to those of a psychological nature, emphasizing the role of virtual communities in normalizing and justifying sexual relationships with children, and encouraging users to engage in this type of offending behavior (Cohen-Almagor, 2013; Holt et al., 2010).

Overall, the aim of the present review is, therefore, to provide an overview of the current knowledge and understanding around the nature of trust development in online networks, and how relationships are formed among members of these, both from a psychological and a criminological perspective, in order to derive insights that may help explain and make better sense of the way users on CSEA forums on the Dark Web communicate and interact with one another. Given the varied focus of the disciplines of psychology and criminology, we thereby hope to offer a more comprehensive overview by reviewing relevant literature from two perspectives.

## 7.2 Method

The literature review presented here employed a systematic search strategy in order to identify any articles that were of relevance to answering the research question. We were predominantly interested in the development of trust and relationships among users on Dark Web networks that are dedicated to CSEA. However, in light of the scarcity of existing studies, articles that explored aspects related thereto on platforms both on and off the Dark Web, and in relation to other cybercriminal activities, were still included. A number of different aspects were identified when reading and re-reading the 21 articles and are synthesized across the studies according to the perspective they represent, thereby offering an insight into the various processes that take place as part of interpersonal communication and interactions on different internet communication platforms.

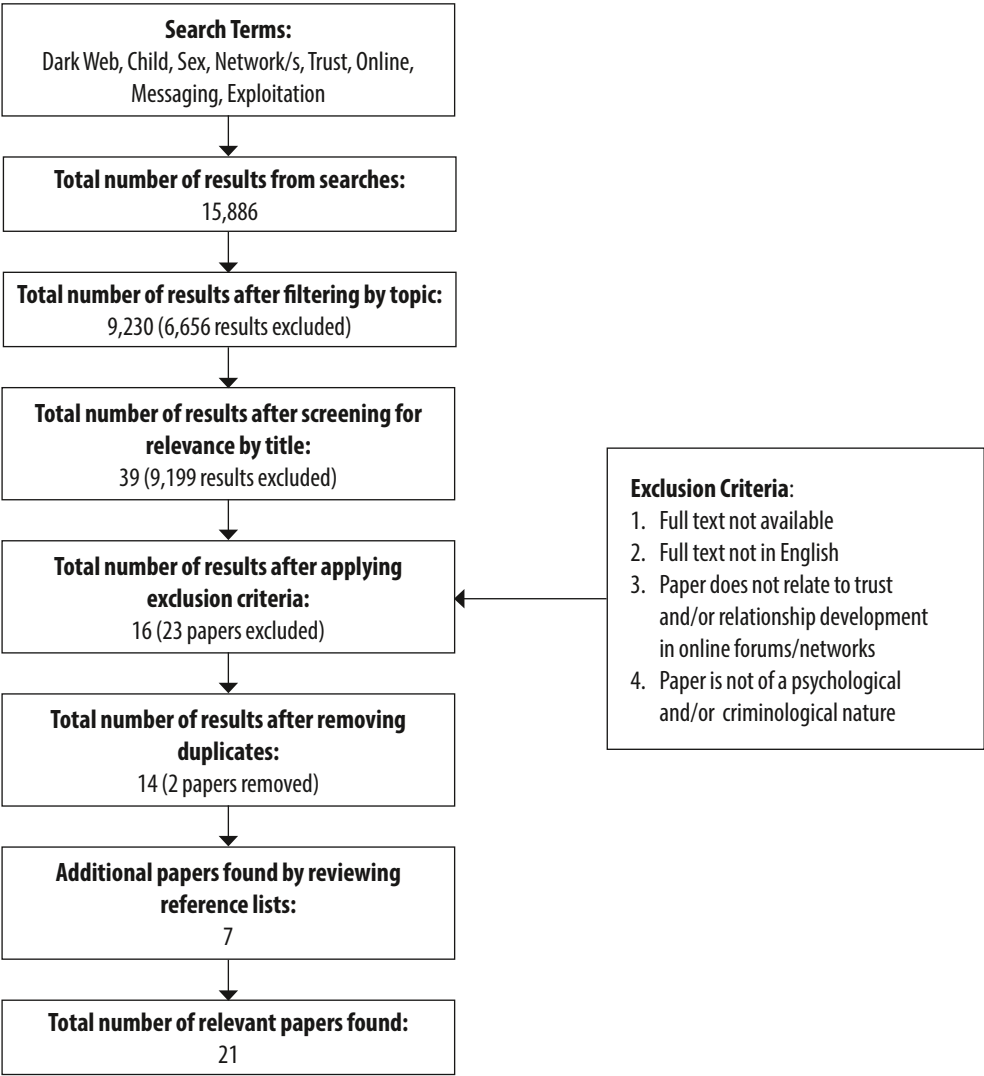
### 7.2.1 Search strategy

Six databases, including Google Scholar, JSTOR, ProQuest, PsycNET, Scopus, and Web of Science, were searched between June 2019 and August 2019 using a combination of different search terms. The search terms centered around the key aspects of the literature review's research question, namely, (i) CSEA, (ii) Dark Web platforms, (iii) online forums and networks, and (iv) trust and relationship development. For databases that allow the filtering of results, the search was limited to the topic areas of psychology, crime, sociology, and social science(s).

### 7.2.2 Search results

A total of 15,886 articles were returned by using several combinations of the search terms. Following the application of filters by topic area (within the databases that allowed this), the number of total articles reduced to 9,230. The titles of these articles were reviewed for relevance, resulting in a further reduction to 39 articles. Once our exclusion criteria were applied, and duplicates were removed, 14 articles remained. Finally, the reference lists of the 14 articles were reviewed, and a further seven articles were identified. This resulted in a final set of 21 articles. Figure 7.1 presents an overview of the steps that were undertaken to achieve the final set of articles included in the review.

**Figure 7.1 PRISMA flow diagram of the systematic literature search**



### 7.2.3 Study characteristics

#### 7.2.3.1 Psychological articles

Of the 21 articles, eight contained a psychological or anthropological focus. Of these, three were conducted in the US and five were conducted in the UK. All except one of the articles were studies that examined qualitative data derived from internet communication platforms, semistructured interviews, or in-depth ethnography (with the

one exception drawing on a range of data from two empirical studies). Two of the eight articles described a thematic and content analysis of a “boy love” support forum, with one article (UK) involving the revisiting of the original study (US). The other two articles from the US examined (i) posts on an internet message board and (ii) threads from web forums, both geared toward individuals with a sexual interest in children. Of the remaining four articles from the UK, one presented a detailed overview of policing online child sexual abuse by drawing on findings from two empirical studies that were conducted between 2003 and 2013, and three involved semi-structured interviews with individuals who had been arrested for or convicted of offenses related to CSEM ( $n = 7 + 13 + 31 = 51$ ). In addition to semi-structured interviews, one study also employed an ethnographic approach that involved 17 months of participant observation ( $n = 81$ ) in a UK group program for individuals who had been arrested for offenses related to CSEM. Table 7.1 provides an overview of the study characteristics of the psychological articles, including study aims, participant details, methodology, and main findings.

**Table 7.1 Overview of study characteristics and main findings from psychological articles<sup>2</sup>**

| Study                  | Aims                                                                           | Participants                                                       | Method & Data Analysis                                                                                                                                                                                                                                                                                                              | Main Findings                                                                                                                                                                                                                                                                                                                                          |
|------------------------|--------------------------------------------------------------------------------|--------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Durkin & Bryant (1999) | To investigate how pedophiles who use the internet account for their deviance. | 41 self-identified pedophiles who participated in an online forum. | 93 posts by 41 self-identified pedophiles were analyzed using content analysis to determine the presence or absence of a number of different variables: (i) account offered, (ii) condemnation of condemners, (iii) denial of injury, (iv) claim of benefit, (v) appeal to loyalties, (vi) BIRGing, and (vii) polythematic account. | Slightly more than half of the participants offered some type of account in defense of pedophilia or adults engaging in sexual activity with children: (i) denial of injury = 39%, (i) condemnation of condemners = 31.7%, (iii) polythematic account = 24.4%, (iv) BIRGing = 14.6%, (v) claim of benefit = 9.8%, and (vi) appeal to loyalties = 4.9%. |

2 In Tables 7.1 and 7.2, we adopted the terminology used in each of the articles. However, we would like to point out that the use of the term “pedophile” may not be accurate in all instances in that some users may not meet the diagnostic criteria for this psychiatric disorder (as part of which an individual experiences a primary or exclusive sexual attraction to pre-pubescent children).

| Study                  | Aims                                                                                                                                                                     | Participants                                                                | Method & Data Analysis                                                                                                                                                                                                                                    | Main Findings                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Holt et al. (2010)     | To investigate the cultural norms that govern pedophile communities, and how individuals become encultured in these online communities.                                  | Five forums run for and by pedophiles with 198, 40, 224, 123 and 418 users. | 705 threads from the five forums were analyzed using inductive grounded theory to draw normative orders which are sets of rules and practices oriented to a common value. The forums were identified and selected through a snow-ball sampling procedure. | Members felt isolated and adopted language emphasizing the separation between them and the outside world. Forums therefore provided a sense of belonging. Members also often discussed sexuality, including fantasies, past experiences or sexual preferences that involved children, and presented with knowledge around legislation and recent policing activity. Members also advised each other on issues of security and how to avoid detection, and offered advice on approaching children online and offline. |
| Malesky & Ennis (2004) | To understand the specific functions of message boards for individuals who make use of them and to investigate the type of cognitive distortions evident in forum posts. | An unknown number of male members of a "boy love" forum.                    | 234 posts over seven days were analyzed using a cognitive distortion checklist with 11 separate categories representing justifications, misperceptions of consequences, attribution of blame to the victim, and supplemental distortions.                 | 27% of posts contained at least one distortion, with euphemistic labelling being the most common distortion and justification (present in 24% of posts). All other distortions were only present in 2-5% of posts. Over 20% of posters were seeking validation of their beliefs, while over 50% provided material such as images and poems relating to boy love. Over 60% of posts contained social elements, with over 50% of posts serving multiple purposes.                                                      |
| Martellozzo (2015)     | To contribute to the field of policing online child sexual abuse, and the development of global police practice.                                                         | 21 officers and forensic examiners.                                         | Online transcripts between offenders and undercover officers, as well as observational notes and interview transcripts from semi-structured interviews, were analyzed using grounded theory to identify and develop themes.                               | Several themes were identified in relation to: (i) the difficulties faced by officers posing as adults with a sexual interest in children and children; (ii) the immersion required to remain adaptable and convincing; and (iii) the community aspect of child sexual abuse forums, with particular reference to a forum where trust was built via engagement and following set rules.                                                                                                                              |

| Study                      | Aims                                                                                                                                                               | Participants                                                                                                                        | Method & Data Analysis                                                                                                                                                                                                                                                                                             | Main Findings                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| O'Halloran & Quayle (2010) | To revisit the forum investigated by Durkin and Bryant (1999), and assess how the forum's nature had changed over 10 years.                                        | 23 contributors to the "boy love" forum with membership ranging from several months to 10 years.                                    | 127 posts by 23 self-identified pedophiles were analyzed using content analysis (using the same template as Durkin & Bryant (1999)).                                                                                                                                                                               | The most common justification was the condemnation of the condemners, followed by denial of injury, claim of benefit, denial of victim, appeals to higher loyalties, and basking in reflected glory. Members who shared their justifications appeared to do so to alleviate feelings of guilt, referring to the forum as a kind of learning environment.                                                                                                                                                                                                                                                                                  |
| Quayle & Taylor (2002)     | To investigate the relationship between those who are sexually interested in children and the internet.                                                            | 13 men convicted of downloading or distributing child sexual exploitation material.                                                 | 13 semi-structured interviews were analyzed using a discursive framework by focusing on the function of interviewees' accounts. Data were subsequently organized into emerging categories based on similarities and differences.                                                                                   | Child sexual exploitation material served the function of sexual stimulation, collecting behavior, escaping real life, and therapy. Only some interviewees used child sexual exploitation material as a method for facilitating social relationships. Trading images via instant messaging enabled the formation of friendships and built networks based on trust. The internet offered a way of creating a private and arousing world.                                                                                                                                                                                                   |
| Rimer (2019)               | To examine child sexual exploitation material users' constructions of children, and childhood online and offline, and explore how these factor in their offending. | 81 men arrested for viewing and possessing child sexual exploitation material, of which 31 took part in semi-structured interviews. | 31 of the sample took part in semi-structured interviews, which employed a 25-question guide split into five sections: background, internet and pornography, children and childhood, and current circumstances. The transcripts and field notes were analyzed using thematic analysis in order to identify themes. | Four themes were identified: (i) constructions of children in the offline world; (ii) constructions of children in the online world; (iii) negotiating "realness": making children anonymous, distant and other; and (iv) negotiating "realness": victim empathy. Participants were found to construct a fundamental difference between children online and in the physical world, with children in images not being perceived as "real" and sexualized. This facilitated offending in terms of overcoming barriers, and allowing participants to hold conventional beliefs about children while engaging in incongruent online activity. |

| Study                 | Aims                                                                                                                      | Participants                                                                                  | Method & Data Analysis                                                                                                                                                                                                                                                                                                                                                                                   | Main Findings                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Winder & Gough (2010) | To understand child sexual exploitation material offenders, and how they rationalize and defend their offending behavior. | Seven convicted child sexual exploitation material users/distributors aged between 20 and 60. | Seven semi-structured interviews were analyzed using Interpretative Phenomenological Analysis. The interview guide centered around family environments, past offenses and feelings about them, the impact of offenders' actions on other areas of their life, other offenses and offender identity, treatment, as well as other individuals committing sexual offenses, and future plans outside prison. | Several key themes were identified in relation to: (i) obsession and compulsion, (ii) isolation, (iii) escapism, (iv) enjoyment, and (v) self-distancing. Most individuals sought to distance themselves from contact sexual offenses/offenders. Individuals also sought to minimize the impact of their actions by construing the offense as an imaginary affair. Following treatment, individuals reported greater accountability for their actions. |

### 7.2.3.2 Criminological articles

Of the 21 articles, 13 contained a criminological focus. Of these, one was conducted in the US, one in Austria, one in Taiwan, two in Australia, and four in Canada and the UK. The majority of the studies ( $n = 8$ ) used naturally occurring, realworld data for the purpose of analysis, including users' forum messages and posts, as well as information about their status, reputation scores, and ratings. Three of these studies used a qualitative approach to data analysis (with one article combining this approach with social network analysis). One study used a quantitative approach, and three used a combination of both. Six studies explored forum sustainability, the distribution and development of user reputation, social and market dynamics on a forum, and trust in general. One study adopted the Event Analysis of Systemic Teamwork (EAST) method, an "integrated suite of methods for analyzing performance and behavior in human-technical systems" (Lacey & Salmon, 2015, p. 121), to investigate the tasks and interactions undertaken by first-time enrollers in illicit markets, as well as trust establishment more broadly. A further two studies conducted interviews with professional experts to establish how users with an interest in CSEA use the internet more generally, and how mechanisms of trust and distrust are addressed in online networks specifically. One other study conducted interviews with drug users and vendors who were active on a specific Dark Web forum in order to examine the similarities and differences between drug dealing on Dark Web markets and drug dealing in the physical world. The interview-based studies used content and thematic analysis for the purpose of analyzing their data. Finally, two articles were literature reviews. Table 7.2 provides an overview of the study characteristics of the criminological articles, including study aims, participant details, methodology, and main findings.

**Table 7.2 Overview of study characteristics and main findings from criminological articles**

| Study                    | Aims                                                                                                                      | Participants                                                                                 | Method & Data Analysis                                                                                                                                                                                                                                                                                                                                                 | Main Findings                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Afroz et al. (2013)      | To investigate what makes a particular forum sustainable, and what distinguishes sustainable forums from those that fail. | Five cybercriminal forums, each of between 8,000 and 19,000 users.                           | An economic framework was applied to examine forum sustainability. The framework considered a number of factors: (i) the monitoring of forum members, (ii) the rate of change of members and their connectivity per month, (iii) the social connections and communication between members, (iv) exclusion criteria, (v) forum enforcement, and (vi) member punishment. | The use of a cheap monitoring system was associated with greater sustainability. This enables the identification of non-trustworthy forum members. In addition, forum growth and connectivity should be consistent and moderate. Less successful forums exhibited staggered growth, with bursts of growth and sudden declines in connectivity. Forums exhibiting a gradual increase in communication were sustainable in light of the growth in social capital and trust building. Forums that use enforcement were also associated with higher sustainability. |
| Broadhurst et al. (2014) | To review a variety of cybercrime organizations, and explore the nature of groups engaged in cybercrime.                  | N/A                                                                                          | The existing literature was reviewed and critically evaluated, drawing on cybercrime typologies, and making reference to existing cybercrime cases, offenders and operations.                                                                                                                                                                                          | A wide variety of organizational structures are involved in cybercrime. The organizations referenced focused on goals, such as freedom of information, defiance of authority, sexual gratification, and technological prowess. A members-only online CSEA group is described to illustrate an example of cybercrime and its offenders.                                                                                                                                                                                                                          |
| Cohen-Almagor (2013)     | To understand how child sexual offenders use the internet, and how to counteract them.                                    | 14 internet experts and senior law enforcement officers in various countries were consulted. | A critical reflection of books, academic papers, news articles, as well as government and law enforcement reports, was conducted, combined with a total of 11 expert interviews.                                                                                                                                                                                       | The internet has enabled the emergence of online communities for the purpose of exchanging information, seeking social support, and meeting desires. The social connections and relationships that are formed encourage trust development. Moreover, sexual interest in children is normalized and justified. Collaboration across various parties is required in order to reduce the threat posed by child sexual offenders.                                                                                                                                   |

| Study                       | Aims                                                                                                                             | Participants                                                                                                                                       | Method & Data Analysis                                                                                                                                                                                                                                                                                                        | Main Findings                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Décary-Héту & Dupont (2013) | To examine how reputation is distributed amongst a single network of botnet hackers, and how it relates to criminal achievement. | One forum with 20,270 members who posted 248,634 public messages was selected and analyzed from February 2007 to November 2011.                    | A custom program was used to download members' account information, posts, reputation scores, and awards received from administrators. A content analysis was conducted on a subset of messages, and a multi-level predictive model was used to establish how reputation was distributed among individual members.            | The model showed that reputation significantly correlated with the number of awards received, time spent on the forum, and size of a member's ego network. Nurturing positive roles and openness led to more sustained levels of reputation, as did engagement in social networking, and helped to reduce mistrust.                                                                                                                                        |
| Dupont (2013)               | To explore the norms and practices that govern the interactions between malicious members online.                                | 113 chat logs between 10 male botnet hackers, who were aged between 17 and 25 years, and any other user, in which malicious hacking was mentioned. | A qualitative data analysis software (QDA Miner) was used to facilitate the coding, annotating and retrieving of the dataset. The data was further analyzed using social network analysis.                                                                                                                                    | Some members were more active than others, however, this was not indicative of social skills or trust. Arguments were also frequent among members. High-trust members often exchanged pieces of code, servers, login details, and warnings. These members also discussed personal issues. Low-trust members shared information, but only to a certain extent, and were more often characterized by failures and ridicule, fostering distrust in the forum. |
| Dupont et al. (2017)        | To explore the social and market dynamics of Darkode, an invite-only cybercrime / hacking forum.                                 | A dataset of 4,788 screenshot files from the forum's discussion threads covering data between 2009 and 2013.                                       | The selection process, through which 344 potential new members introduced themselves to the community in order to be accepted into the forum, was examined using a qualitative approach in order to determine whether a rigorous procedure significantly enhanced trust and contributed to the efficiency of the marketplace. | Despite the security-minded reputation of the forum, many members were let in for profit. Trust and reliability therefore remained elusive, and interactions were often fraught with suspicion and accusations. It was concluded that high-end markets also face distrust.                                                                                                                                                                                 |

| Study                | Aims                                                                                                                                                   | Participants                                                                                                                                                                                              | Method & Data Analysis                                                                                                                                                                                                                                                                                                                                                                                                                        | Main Findings                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Dupont et al. (2016) | To investigate how trust (as measured by a reputation system) is distributed in quality and quantity between members, and how it fluctuates over time. | A large hacking discussion forum of 29,985 hackers (20,768 general hackers, and 9,127 botnet hackers) who had been rated by 9,177 other members through 449,478 different events, over a 27-month period. | A qualitative analysis was conducted of 25,000 feedback comments in order to examine whether they were a positive or negative evaluation on (i) the business relationship, (ii) someone's contribution, (iii) an assessment of an individual's interaction with the feedback provider, (iv) their technical ability, (v) humorous, sarcastic or absurd comments on a member's actions or skills, and (vi) unreadable or meaningless comments. | The variation in positive feedback was attributed to the different natures of the groups, with botnet hackers being involved in a market-based community where members have more to lose. There was a bias towards reporting positive outcomes which reduced the utility of the ratings, as did the low participation rate in the rating system. The qualitative analysis revealed that trustworthiness was mostly grounded in humor and sarcasm. |
| Hsu et al. (2011)    | To examine the antecedents of trust in virtual communities.                                                                                            | 324 members of tech-related virtual communities, 244 of which were male, and 80 of which were female.                                                                                                     | Surveys were distributed, including questions on knowledge growth, perceived responsiveness, social interaction ties, shared vision, system quality, knowledge quality, trust in the system, and knowledge-sharing intentions. A research model was tested, using structural equation modelling, to examine the influence of each factor on other connected ones.                                                                             | Shared vision, perceived responsiveness and knowledge growth had significant effects on trust in members, while knowledge quality had a significant effect on trust in the system. Moreover, trust in the system and its members significantly affected members' knowledge-sharing intentions.                                                                                                                                                    |

| Study                 | Aims                                                                                                                                                      | Participants                                                                                       | Method & Data Analysis                                                                                                                                                                                                                                                                                                                                                                                                                                | Main Findings                                                                                                                                                                                                                                                                                                                                                                                                       |
|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Lacey & Salmon (2015) | To investigate the tasks and interactions undertaken by first-time en-rollers on illicit markets, and trust establishment between them and other members. | The Republic of Lampeduza (a carding forum) with over 4,000 trusted members and over 71,000 posts. | Event Analysis of Systemic Teamwork (EAST) was used to describe the goals and future tasks performed by members of a system, the organization, and communications between members, as well as how information is distributed across members in a system. The researchers conducted a hierarchical task analysis (HTA) to break down the enrolment process into smaller goals and plans, and observed all steps involved in registering and enrolling. | The HTA revealed three key steps with multiple sub-steps. A key trust-building step was the allocation of an unknown reviewer who specifies the trust-building requirements. The communication and organization analysis revealed a complex network involving non-human and human components. The information network analysis indicated that quality assurance is of high importance in trust-building strategies. |
| Lusthaus (2012)       | To investigate the mechanisms by which cybercriminals address the issue of distrust in online networks.                                                   | Nine internet security practitioners, law enforcement officers, and cybercriminals.                | Interview data were considered alongside legal documents, security firm reports, and media articles. All interviews were audio-recorded, transcribed and analyzed using thematic analysis.                                                                                                                                                                                                                                                            | Prospective cybercriminals must present a criminal identity as a key step in trust development. These identities can be tested via background checks, criminal acts, and information hostages. To assess the attributes of a prospective cybercriminal, existing forums use criminal displays, referrals and expertise demonstrations. Enforcement measures are also employed.                                      |

| Study                    | Aims                                                                                                                                                            | Participants                                                                              | Method & Data Analysis                                                                                                                                                                                                                                                                      | Main Findings                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Nurse & Bada (2018)      | To examine the group dynamics of cybercrime forums from several perspectives.                                                                                   | N/A                                                                                       | The existing literature was reviewed and critically evaluated, drawing on online platforms used by cybercriminals, the types of groups present (including their motivations and actions), and how these groups form and operate.                                                            | Cybercriminal groups have different structures and goals. Trust in online groups is characterized by the integrity of the system to maintain anonymity, and can be directed to the community, information sources, potential partners, and authorities. Many forums use screening measures to test trustworthiness of members. Individuals have to strike a balance between changing nicknames in order to distance themselves from past crimes, and revealing certain aspects of their identity for the purpose of building a reputation and attracting criminal collaborations. |
| Tzanetakis et al. (2016) | To examine the similarities and differences between drug dealing offline and on Dark Web markets in terms of violence, trust and the logistics of distribution. | 214 “conventional” drug users and/or dealers and four vendors on the online market Agora. | Participants took part in interviews as part of an existing mixed-method research project. Qualitative case studies were conducted with the Dark Web vendors, considering data such as customer feedback, profile pages, and forum chat material, and were analyzed using content analysis. | Trust in online networks was proactively promoted in order to increase cooperation and sales, and attract new customers. Vendors’ ratings and conflict resolutions help to build a trustworthy reputation. Trust is therefore characterized by network structure and good conduct. In offline communities, trust was more based on interpersonal relationships. Third-party conflict resolution was more common in online communities.                                                                                                                                            |

| Study             | Aims                                                                                                                                                                                    | Participants                                           | Method & Data Analysis                                                                                                                                                                                                                                                                                                                                                                     | Main Findings                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Yip et al. (2013) | To examine the structure of organized cybercrime, and explore the facilitation of trust using theories derived from social psychology, organized crime, and transaction cost economics. | Data from public discussions on online carding forums. | Theories of transaction cost economics were applied to data from shut-down online markets and carding forums. Uncertainty was treated as a cost to the transactions, and was therefore used as the unit of analysis, in order to examine the mechanisms cybercriminals use to control two-key sources of uncertainty: (i) the quality of merchandise, and (ii) the identity of the trader. | To mitigate uncertainty and facilitate trust, discussion forums adopt a hybrid organizational structure. Quality assurance via reputation systems was one method used to increase institutional trust. However, social networking was the main means through which interpersonal trust between members was increased. Through exchanges, members learn good conduct and group rules, and shared personal information and feelings towards their profession and any associated risks. Having a forum built on interpersonal and institutional trust is therefore imperative for success, as this reduces transactional cost and allows forums to grow. |

**Table 7.3 Summary of critical findings**

| Critical Findings         |                                                                                                                                                                                                                                                                                                                                             |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Psychological Literature  | <ul style="list-style-type: none"> <li>- Online communities and networks serve various functions, including validation and support, as well as advice, guidance, and information</li> <li>- Users of online platforms appear to meet social and interpersonal needs, including connecting and building relationships with others</li> </ul> |
| Criminological Literature | <ul style="list-style-type: none"> <li>- The establishment of trust and relationships is accomplished through social and technical mechanisms and is directly related to forum users' online identity</li> <li>- Once trust is established, it is maintained through the social aspects of dedication to the community</li> </ul>           |

## 7.3 Results and discussion

### 7.3.1 Marginalization and semantic manipulation

In the study by Holt et al. (2010), users clearly recognized that their sexual interests and preferences were different from the wider population, which carries with it mar-

ginalization and social stigma. Some described fearing for their personal safety and being persecuted. Within this context, users sought to distinguish between individuals who engage in various sexual behaviors involving children. More specifically, there is a group of users who proclaim that they love children and would never hurt them (often referred to online as “child lovers”); there is another group of users who are open about engaging in the sexual abuse of children (often referred to as “pedophiles”). The former actively attempt to distance themselves from the “pedophile” label and view themselves as different and not harming children. Semantic manipulation by means of differentiating between “child lovers” (whose attraction to children is portrayed as a romantic relationship) and “pedophiles” is clearly important for the former in terms of preserving a positive self-concept (Holt et al., 2010).

### **7.3.2 Justifications for engaging in offending behavior against children**

Malesky and Ennis (2004) analyzed users’ posts on an internet message board with a particular focus on distorted thinking that was supportive of offending behavior involving the sexual abuse of children. the term “cognitive distortions” is often used in the literature to refer to a very broad range of both postoffense explanations, and cognitive processes during offending, including excuses, rationalizations, beliefs, perceptions, justifications, denials, minimizations, and defenses (Maruna & Mann, 2006; O’Ciardha & Ward, 2013). Firstly, commonly held attitudes and beliefs that functioned to strengthen users’ attempts at building a credible argument in defense of pedophilia (i.e. a sexual interest in children) related to (i) denial of injury to children, (ii) denial of victim, (iii) claim of benefit, and (iv) condemning the condemners (i.e. discrediting others who challenge them) (O’Halloran & Quayle, 2010). The dominance of justifications over excuses in O’Halloran and Quayle’s (2010) study suggests that users did not consider that sexual contact with children was wrong, but merely that it is viewed negatively by wider society. The sharing of these justifications was found to be an important part of discussions that featured on the support forum the authors analyzed.

Secondly, participants in Quayle and Taylor’s (2002) and Winder and Gough’s (2010) studies claimed that accessing CSEM for the purpose of sexual stimulation, arousal, and gratification, often accompanied by masturbatory activity, acted as (i) therapy for dealing with negative emotional states, such as loneliness, depression or relationship breakdowns; (ii) a substitute for committing contact sexual offenses in the physical world; and (iii) a safe outlet for feelings that would otherwise lead to a contact sexual offense. For others, it arguably acted as a blueprint and stimulus for a contact sexual offense, while some participants maintained that preventing masturbation was “accentuating the problem by provoking more contact offenses” (Quayle & Taylor, 2002, p. 131).

Further justifications commonly reported in the studies that involved interviews with individuals who were convicted of offenses related to CSEM include (i) that it is “just pictures” (Rimer, 2019); (ii) drawing comparisons between image offenses and contact sexual offenses (e.g. “I am just looking,” “nobody is getting harmed”; Rimer, 2019; Winder & Gough, 2010, p. 130); (iii) referring to children in the images as being happy and smiling; (iv) experiencing sexual abuse themselves; (v) citing legislation in other countries, where age of consent is such that it legalizes the sexual behavior engaged in by the individual; and (vi) claiming that the production of imagery offers employment for children in particularly poor parts of the world, without which children would starve (Quayle & Taylor, 2002; Rimer, 2019; Winder & Gough, 2010). In addition, participants in the Rimer (2019) study constructed children depicted in CSEM as sexualized and less or not real, which is partly facilitated by the anonymous nature of the online environment (and the fact that they are unknown to them). This therefore allows individuals who view this type of material to objectify children, and become desensitized, detached, and distanced to the content, which assists in the overcoming of barriers, and enables the continued engagement in offending behavior (Rimer, 2019).

Participants also commonly described the process of accessing CSEM as addictive and compulsive. This not only implies a loss of personal agency, but also allows users to present their behavior as out of their control (e.g. “I can’t help myself”), absolving them of culpability (Quayle & Taylor, 2002). Similarly, participants in Winder and Gough’s (2010) study presented their offending in the context of being driven by obsessions and compulsions, thereby elevating “the role of psychological illness over personal choice and culpability, while isolation privileges a situational over an individual explanation” (p. 128–129). Through talking about CSEM by highlighting its addictive and compulsive properties, it serves to distance the user from the material and both minimizes and removes any personal responsibility.

Overall, this is largely facilitated by the perceived noncontact nature of offenses related to CSEM, with images being described as “mundane and innocuous” (Winder & Gough, 2010, p. 129) to negate their severity. Participants further claimed that children smiling in images indicated that they were happy and that victims who were not aware of being recorded were not harmed. Furthermore, they distanced themselves from the label and identity of “sexual offender,” denying that they were any danger to children, and presenting offenses related to CSEM as less wrong and harmful than contact sexual offenses. Another attempt to justify their offending behavior was by means of the “looking-but-not-touching” mitigation, implying no knowledge of or contact with the child depicted in the material (Rimer, 2019; Winder & Gough, 2010).

Participants who referred to the accessing and downloading of CSEM as the main

motivator for using internet communication platforms made little to no reference to the fact that this material depicts vulnerable children, but rather drew comparisons with other commodities that are known for collecting behavior (e.g. stamps). Collecting further facilitates the objectification of children, given that images in this context are treated as currency (Quayle & Taylor, 2002). It is of note that those who were engaging in this type of behavior not only collected CSEM but also other forms of pornography, despite presenting with a sexual interest in children. Others described the progression and escalation from legal adult pornography to seeking out more novel and extreme material (i.e. CSEM) (Quayle & Taylor, 2002; Rimer, 2019).

### **7.3.3 Function of online communities and networks**

Given that individuals with a sexual interest in children represent a marginalized group, online communities serve the function of offering support by, and understanding from, like-minded individuals in various ways (Holt et al., 2010; Martellozzo, 2015). Holt et al. (2010) considered the role of such communities in developing a so-called “subculture” of “pedophiles,” as part of which attitudes, beliefs, and justifications are fostered that support relationships with children. The authors concluded that “prominence placed on marginalization may act as a primer in individuals’ behavioral chain, freeing them to offend as they are already social outcasts” (Holt et al., 2010, p. 21). Furthermore, through facilitating connection with like-minded individuals, online communities create an environment in which individuals’ attitudes, beliefs and behaviors are normalized, validated, and even minimized. This is particularly powerful for those who are seeking to come to understand their sexual interests of or attraction to children (Martellozzo, 2015), and ultimately achieves social cohesion and a sense of belonging among individuals (Holt et al., 2010). In their study of an online discussion group, Holt et al. (2010) found that many of the conversations that took place on it resembled daily catchups, with users telling each other about their day and what they were up to. Furthermore, according to Ward and Hudson (2000), offenders with a sexual interest in children gravitate toward environments with like-minded individuals who hold similar attitudes and beliefs that support their lifestyle and belief system.

More specifically, the largest percentage of posts (63%) in an analysis of an internet message board fell into the category of communications that were social in nature and did not specifically involve content related to “boy love” (Malesky & Ennis, 2004). In addition, slightly more than one-fifth of the posts were classified as validating pedophilic beliefs and relationships. One may argue that users did not feel compelled to defend their beliefs to themselves or others through cognitive distortions, and felt relatively accepted in the community, which may be expected given that it was geared toward users with an interest in “boy love,” and likely attracted like-minded individu-

als. The authors concluded that users may find a sense of membership and community through participation in and interaction on platforms online, including connecting with others and building relationships. Especially for those who are potentially marginalized in their communities, or society more broadly, this may lead to feelings of empowerment. Seeking out and joining online communities therefore clearly serves the function of social connection, particularly where this is absent and missing in someone's personal life in the physical world. In addition, online networks may also provide an opportunity for users to excel at something, achieve a particular status in the community, and gain the respect of others. This is especially powerful where users' identities in the physical world bear little resemblance to the identity they have created online. In particular, users described creating a secret and separate world to their reality, which for some took on the role of a fantasy in comparison to their mundane everyday life. The element of danger and illegality in such cases acted as an excitement and escape (O'Halloran & Quayle, 2010).

In addition to meeting the more social and interpersonal needs of users, online communities geared toward individuals with a sexual interest in children also serve the purpose of facilitating access to advice, guidance, and information. This may be related to (i) approaching children (both online and in the physical world), (ii) initiating and developing friendships with children, (iii) gaining access to potential victims (for sexual abuse in the physical world, including the production of CSEM), and (iv) sharing "best practice" and "what works" with regard to all of these, as well as achieving compliance in victims, ensuring non-disclosure, concealing one's identity, and avoiding detection overall (Holt et al., 2010; Martellozzo, 2015).

To practice security and avoid detection, much of the content of the conversations in Holt et al.'s (2010) study focused on advice around carefully managing personal information and activities, as well as being mindful of the level and type of information contained within posts, and where these are posted. For example, some users may present their experiences as dreams or fantasies (rather than actual acts or activities they engaged in or happened). Other advice would center around privacy issues and technical requirements in order to protect users' true identities and keep their equipment secure. Restrictive guidelines around what content was allowed to be posted or published helped to minimize negative attention for the platform, including in relation to the exchange of illegal material. Throughout, the conversations were accompanied by users' concerns around safety and the law, clarifying definitions of what is legal and illegal. They further expressed their opinions about what they perceive to be harmful to children (or not), and whether CSEM represents contact sexual offending, debated about whether children are able to consent, and discussed recent cases, arrests, and prosecutions of individuals involved in CSEM (Holt et al., 2010).

Finally, online communities follow established group dynamics and hierarchies of status, expertise, and apprenticeship (O'Halloran & Quayle, 2010). According to Martellozzo (2015), some of these may be compared to organized criminal organizations, whereby members are required to present with certain personal qualities in order to gain membership status (such as honesty, honor, obedience, and participation). More specifically, "membership was reinforced by having material to trade, by behaving correctly, and by following the rules for trading. Once status had been achieved through membership of the group, trading reduced, and, instead, the social function of the online exchanges, and the ability to be on the inside and obtain special photographs, was more important" (Quayle & Taylor, 2002, p. 346). As noted previously, within online communities, imagery may therefore act as a medium for exchange, whereby users may look to build a large collection, complete a series of images, and thereby look for missing parts, as well as distributing new material, which ultimately contributes to their standing in the community (in terms of the nature of the material, its size, completeness, and value, with participants in Quayle and Taylor's (2002) study referring to some images as "Picassos").

The forming of social relationships and establishment of social cohesion among a group of users is further facilitated by this very exchanging and trading of imagery, which requires users to come into contact with others who are similarly interested in, and engage with, this type of material (Quayle & Taylor, 2002). The possession of imagery was often also a requirement for joining and becoming a member of a community or forum. Connections or friendships with certain users may also advance the status of another, while at the same time facilitating access to their collection and victims. Imagery was often described as currency that enabled the building of one's reputation and trust with other users, contributing and helping to maintain relationships with them. In Quayle and Taylor's (2002) study, participants also referred to the importance and prioritization of relationships over imagery, describing the community as something like a club, whereby users were provided with and given what they were looking for and wanted, while ensuring that the forum was running smoothly. The exchange of imagery was therefore contextualized as a commodity that enabled social cohesion.

Overall, being a member of one of these online communities creates a sense of belonging to an in-group, which works to establish elements of trust and "being in it together." According to Martellozzo (2015), trust is further developed through engagement and following set rules. Members who otherwise feel oppressed by wider society in the physical world are immersed in a strong social network online, as part of which users may share their likes and dislikes, sexual interests and preferences, as well as their daily encounters or experiences. Holt et al. (2010) concluded that "by

sharing information with others in an environment where feedback, reciprocity, and a congruence of opinion, can be found, the forum users are able to connect in ways that validate and support their actions” (p. 20).

Given the nature of online networks that center around CSEA, including its material, it is to be expected that a certain level of trust among users is established through mere association with and involvement therein. Being a member of an online community thereby gives users the impression of being part of an in-group, which works to reinforce one’s perception that they are “in it together,” and “them against us.” In fact, this raises important questions in terms of the power these online networks have in contributing to the escalation of offending behavior, both with regard to acceleration and aggravation (O’Halloran & Quayle, 2010); they provide access to expert advice, guidance, and information, including how to find victims or particular material, as well as detailed descriptions of various *modi operandi*, and how to avoid detection (Woodhams et al., 2021). Arguably, receiving support from like-minded individuals in the way it has been described here is suggested to promote pro-offending beliefs in socially isolated individuals (O’Halloran & Quayle, 2010). Interactions as part of online communities provide immediate positive reinforcement for users, and their narratives can take the form of either excuses or justifications that aim to minimize questionable activity.

It is important to highlight how difficult it is to verify users’ true intentions behind what they post (O’Halloran & Quayle, 2010); they may provide certain content to comply with rules and regulations, or to seek acceptance, recognition, and status within the network. In order for trust to be established and maintained, and for a platform to remain secure, users may merely be able to join a network and become a member by being invited or meeting specific criteria. This not only prevents law enforcement from infiltrating the network but also ensures that only users who are serious about becoming members join the community.

#### **7.3.4 Trust establishment in online and offline communities**

Trust is established differently in online and offline environments. In offline environments, trust may be developed through previously existing ties, personal bonds, common interests, and values, as well as face-to-face encounters. However, these are largely lacking in online environments, and the challenge is therefore that trust has to be established under anonymity without knowledge of who one’s co-offender is, making it fragile and difficult to sustain (Décary-Héту & Dupont, 2013; Dupont et al., 2016; Tzanetakis et al., 2016). Nevertheless, users have to trust both one another (to be willing to share information and co-offend), and the reliability of the (technological) system, including its standards and mechanisms (Hsu et al., 2011).

On the one hand, the anonymous nature of the online environment affords users protection against exposure and a place where they can engage in conversation and interaction, making it suitable for supply to meet demand and the exchange of technical expertise (Nurse & Bada, 2018). On the other hand, anonymity hinders the process of trust establishment and development (Dupont et al., 2016, 2017; Lusthaus, 2012). Those who engage in offending behavior online therefore have to carefully balance between masking their identity to avoid exposure and detection, and revealing elements of it for the purposes of criminal cooperation (Lusthaus, 2012; Nurse & Bada, 2018).

### **7.3.5 Trust establishment in Dark Web communities**

The additional layers of anonymity afforded by the Dark Web make the process of trust establishment and development even more challenging. Dark Web communities are uncertain and risky environments by default (Nurse & Bada, 2018; Yip et al., 2013), and are often frequented by users or outsiders who try to attack them, thereby undermining and endangering their existence. In order for a Dark Web forum to be successful, a balance between negative sentiment and distrust and an environment characterized by “good” behavior is required (Décary-Hétu & Dupont, 2013). More specifically, trust establishment in CSEA networks on the Dark Web is further complicated in light of the sensitive nature of the topic area. Betrayal by a trusted co-offender, or identification by law enforcement personnel who pose as a co-offender, are associated with serious risks, such as detection and exposure, which ultimately creates a structural deficit in terms of trustworthiness (Dupont et al., 2016; Dupont et al., 2017). One may therefore argue that most ties in criminal networks online are not based on strong interpersonal relationships and social capital (as is the case in criminal networks in the physical world), but that they are sufficiently strong to provide access to sought-after resources. According to Yip et al. (2013), trust is never guaranteed and remains a vulnerable entity; it is maintained and further developed by progressing through various stages.

### **7.3.6 Initial identity construction and trust development**

In criminal networks online, and more specifically in CSEA networks on the Dark Web, a user does not tend to have an established identity in the beginning. However, in order to develop collaborative ties, and become an accepted (and eventually trusted) user, a user’s identity needs to be established over time. Open networks are therefore convenient locations for the sharing and learning of new skills, socializing, and meeting new people, as well as for the initiation of trust development to begin (Dupont, 2013). Dark Web forums, however, place emphasis on new members to demonstrate their legitimacy and reliability (Lacey & Salmon, 2015). Lusthaus (2012) suggests that

forums formally or informally assess cybercriminal attributes to establish a baseline for cooperation. This may be achieved by means of (i) background checks, (ii) referrals, (iii) transcripts of previous communication, (iv) evidence of past criminal activity, and (iv) exchange of compromising information. In the same way as some of these cybercriminal forums require the provision of evidence of legitimacy and reliability, CSEA forums on the Dark Web may request CSEM for a user to join the network or to continue their membership (Broadhurst et al., 2014; Lusthaus, 2012).

This initial contact is a first step in the establishment of an online identity, which is a personal brand, and lays the foundation for a reputation that is necessary for trust to be developed further (Lusthaus, 2012; Yip et al., 2013). Reputation is one of the most important elements in being seen as a trustworthy co-offender (i.e. a precursor for trustworthiness) (Décary-Héту & Dupont, 2013; Dupont et al., 2016). In CSEA forums on the Dark Web, members may achieve a higher status based on the quantity and quality of their contributions, which are delivered by their usernames and therefore intrinsically tied to their online identity. Members may further be rewarded for producing and sharing new CSEM (Broadhurst et al., 2014). Here, a dilemma becomes apparent – while one's identity, reputation, and trustworthiness are associated with a username, there is a competing incentive to periodically change it in order to avoid law enforcement detection and exposure (Lusthaus, 2012; Nurse & Bada, 2018).

### **7.3.7 Maintenance of trust**

Users who aim to establish a reputation, and sustain the cooperation with a trusted co-offender, may choose to reveal personal characteristics and engage in social and networking behaviors to support this process. Behavior deemed to be trustworthy involves portraying oneself as an active user by engaging in frequent activity, including posting messages, contributing to open discussions, exchanging valuable advice and knowledge (e.g. through tutorials), and generally being helpful, as well as mentoring and offering feedback to others (Afroz et al., 2013; Décary-Héту & Dupont, 2013; Tzanetakis et al., 2016; Yip et al., 2013). In addition, research indicates that humor, playfulness, and sarcasm are frequently used to invoke trustworthiness (Dupont et al., 2016), and that it is the commitment and dedication users show to the community which leads to a mutual sense of belonging and trust. Social skills, such as the ability to establish and maintain a good quantity and quality of interpersonal ties, are crucial in the search for suitable co-offenders (Dupont, 2013). It is here where an in-group identity may be formed which lays the foundation for informal social control (Yip et al., 2013).

For some users, establishing a good reputation and trustworthiness may become a goal in itself, and they present with the explicit desire to achieve status by moving up

the ranks in a forum (Décary-Hétu & Dupont, 2013; Lusthaus, 2012). While the primary motivation for users of CSEA forums on the Dark Web may be sexual gratification, competing for a higher status within the community is equally important in light of the associated benefits (Broadhurst et al., 2014). Trustworthiness and reputation may therefore be achieved through a combination of personal characteristics (i.e. who you are), networking characteristics (i.e., who you know), and behavioral characteristics (i.e. what you do), which need to be maintained over time, and cannot be easily feigned (Décary-Hétu & Dupont, 2013).

Once trust has been established, it must be maintained. Here, the social aspect becomes valuable – dedication to the community through engaging in frequent activity and communication (especially by sharing new and unique CSEM), unconditional cooperation, exchanging advice and knowledge, and generally being helpful and humorous, are all ways to achieve this, and are rewarded with recognition by others. Emphasis is therefore placed on a friendly atmosphere that is characterized by good behavior and politeness, appreciation, and respect toward one another (Afroz et al., 2013; Broadhurst et al., 2014; Décary-Hétu & Dupont, 2013; Tzane-takis et al., 2016; Yip et al., 2013). Long-term trust, as in the physical world, is largely related to social skills, such as repeated interaction and familiarity, and general comradeship (Cohen-Almagor, 2013; Hsu et al., 2011). Ultimately, a well-functioning network in which users get on and respect one another also make it stronger and more successful, eventually developing resilience to deterioration (Dupont, 2013). Through facilitating the formation of trusting and meaningful relationships, most users will still exchange illegal material and co-offend on CSEA forums on the Dark Web, despite the risks this involves (Cohen-Almagor, 2013; Dupont et al., 2016; Lusthaus, 2012; Yip et al., 2013).

### **7.3.8 Limitations and directions for future research**

While the review has demonstrated that asking a question of the literature that combines two different perspectives is valuable for a more in-depth understanding of the topic area, a number of limitations have to be acknowledged. Naturally, studies from different disciplines vary in terms of their methods and approaches to data analysis, which impacts on the comparability across the included articles in our review. However, within each disciplinary set of included articles, studies were comparable in terms of the research questions they posed, and the methodological approaches used to address these. Nevertheless, it was noted that the qualitative approaches to data analysis were often not specified or described in the necessary detail in the criminological literature.

While both the psychological and the criminological literature lacked a focus on

CSEA forums on the Dark Web, they still considered important aspects that are related to and underpin the formation of trust and relationships among users in online networks. More specifically, it became apparent that most psychological studies had been conducted with datasets that were derived from the Surface Web or samples of individuals who had been arrested for or convicted of offenses related to CSEM. None of the articles therefore specifically referred to data that had been derived from, or users that had been involved in, networks on the Dark Web. Given that most of these studies were completed between 1999 and 2015, this is perhaps to be expected. Interest in the Dark Web, and its use for illegal purposes, has received relatively little attention until 2017, when the international law enforcement operation by Taskforce Argos first offered an insight into the wide-ranging role the Dark Web played in the commission of offenses related to CSEA.

The literature would therefore benefit from a more in-depth examination of the process through which individuals seek to establish trust, and develop relationships, with other users on CSEA forums on the Dark Web. It would be of interest to explore how individuals describe this process, as well as which aspects and features they (perceive to) take into consideration when making the decision of whether or not another user is trustworthy enough to initiate contact and develop a relationship with. Further research is also needed in terms of better understanding this population from a psychological perspective. In addition, it would be useful to explore in more detail how trust-based personal relationships between co-offenders may trigger the formation of smaller sub-networks (within larger CSEA networks on the Dark Web), and how this may contribute to the progression and escalation of offending behavior. It goes without saying that the absence of such studies is at least in part due to the immense difficulty of accessing data derived from such forums.

**Table 7.4 Summary of implications for practice, policy, and research**

|          | Implications                                                                                                                                                                                                                                                                                                |
|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Practice | <ul style="list-style-type: none"><li>- Users' motivation for accessing online platforms is predominantly of a sexual nature</li><li>- Users with a sexual interest in children experience marginalization and social stigma, sometimes fearing for their personal safety</li></ul>                         |
| Policy   | <ul style="list-style-type: none"><li>- Law enforcement having to meet increasingly more difficult to achieve criteria to join particular networks</li><li>- Knowledge around how users operate benefits law enforcement for the purpose of early detection, and informing operational strategies</li></ul> |
| Research | <ul style="list-style-type: none"><li>- To better understand individuals who interact on Dark Web networks that are geared toward the sexual exploitation and abuse of children</li><li>- To explore the role of online networks in the escalation of offending behavior</li></ul>                          |

## 7.4 Conclusion

The review presented here aimed to provide an overview of the current knowledge and understanding of the nature of trust and relationship development among members of online networks that are dedicated to CSEA, both from a psychological and a criminological perspective. While the two disciplines vary in their focus, they share an interest in the topic. We were particularly interested in deriving insights from a larger literature base that may help us explain, and make better sense of, the way users on CSEA forums on the Dark Web communicate and interact with one another. The psychological literature is predominantly concerned with individuals' motivations and the function their behavior serves, whereas the criminological literature concerns itself more with how individuals interact online. We therefore sought to answer the question of how users develop trust and relationships in a high-stakes environment (in terms of one's identity and actions being revealed) that is predominantly used for illegal purposes, and where levels of information about others and their trustworthiness are limited.

Further contributing to our existing knowledge and understanding of this phenomenon is important in light of the implications for law enforcement and policy. Law enforcement would benefit from a more established evidence base in terms of better understanding how users operate on such networks, not only for the purpose of early detection but also in order to inform operational strategies around undercover policing. Industry in the form of public and private companies also have a vested interest in keeping up-to-date with current knowledge and understanding around the use of internet communication platforms for illegal purposes, given their role in the monitoring of illegal content, as well as its identification and removal.



CHAPTER 8

# GENERAL DISCUSSION AND CONCLUSION

## Chapter 8: General discussion and conclusion

This chapter presents the conclusions of this dissertation. The scientific objective of this dissertation was to describe and explain the criminal process and offender behavior on child sexual abuse material (CSAM) fora on the Darkweb using a quantitative as well as a qualitative approach. The practical relevance of this exercise is that the results of the research inform professionals working in areas such as law enforcement, offender management and treatment and probation services about a previously hidden population that they may come across in their future work. The research questions, as outlined in Chapter 1, are:

1. How can the criminal process of Darkweb CSAM fora be characterized?
2. How organized is the crime of CSAM on the Darkweb?
3. Which offender profiles and behavioral patterns can be distinguished on Darkweb CSAM fora?
4. How can keyplayers on Darkweb CSAM fora be identified?
5. How is trust on Darkweb CSAM fora established?

This final chapter summarizes and critically reflects on the main findings of the six empirical studies that make up this dissertation, provides an appraisal of methodological strengths and limitations, and discusses several specific implications for policy and practice, along with suggestions for future research.

### 8.1 Main findings

The main findings will be presented organized along the lines of the research questions. The conclusions for each research question will be discussed using the results of the various papers presented in this dissertation. The first and broadest research question will be elaborated upon extensively as the answer to this question sets the basis for the following research questions.

#### 8.1.1 How can the criminal process of Darkweb CSAM fora be characterized?

In order to contribute to the knowledge on the steps involved in the criminal process of Darkweb CSAM offending, Chapter 2 provided a crime script analysis (Cornish, 1994), using a large sample of the communication data of four CSAM Darkweb fora and suspect interviews of a Darkweb offender who was the administrator on one of these fora for cross-validation. A content analysis (Braun & Clarke, 2006) of forum

posts and threads resulted in a step-by-step description of the criminal process, distinguishing four successive phases.

In the first phase, preparations necessary to access the Darkweb CSAM forum are being made. Building a Darkweb forum, but also merely accessing it, does not occur incidentally, and asks for certain technical and motivational preparations. Second, when members enter the forum for the first time – the preactivity stage –, they start with creating an online identity, introducing themselves by disclosing their nickname and past and current experiences with and fantasies about child abuse. This creates an open atmosphere characterized by a sense of belonging in which the boundaries between the legal and illegal easily become blurred. The third phase, the activity stage, consists of the actual execution of the main illegal act of exchanging CSAM. Members are actively encouraged by other members to contribute to the forum by posting messages, images, and videos and by taking the time to respond to others and to reply to questions asked. Finally, the postactivity stage consists of behaviors of safely and securely exiting the crime scene and preventing detection. Some overall and more general findings regarding this criminal process are worth mentioning.

When describing the criminal process, findings of various chapters in this dissertation suggest that a distinction between keyplayer members and general forum members has to be made, because of major differences in their role and behavior on the forum. Keyplayer members often have a higher forum status, such as moderator or administrator, but they could also be ‘regular’ forum members who carry out important forum tasks. Keyplayers are much more active, and often play a role in services important to the forum’s establishment, maintenance and management. Keyplayers for instance make sure that the forum environments are organized in a logical way, and that forum members place their content in the right locations. Moreover, they offer other forum members guidance in issues such as safety and security and they are often involved in the forum’s branding and marketing. Contrarily, general forum members primarily use the forum’s infrastructure for the exchange of CSAM and sometimes to communicate with like-minded others, but their role and activity is not pivotal for the forum’s existence and development.

Another general finding, leading from Chapter 2, is that the most important characteristic of the criminal process of Darkweb CSAM offending is the continuous focus on technical security and support. The importance of acquiring or sharing sufficient technical knowledge (for example in the form of tutorials) is highlighted in all four stages of the crime script. This can partly be explained by the growing number of offenders active and images exchanged on the Darkweb (Goodman, 2015; Bleakley, 2018; Leclerc et al., 2021; Owens et al., 2016; Woodhams et al., 2021). The more traffic to and activity on CSAM fora, the more security-related mistakes are likely to be made by

forum members. Novice forum members therefore continuously need to be tutored in basic technical practicalities. Moreover, fora are under continuous threat, for example in the form of law enforcement interference and hacker attacks who may perform DDoS attacks or spam the forum website. This places a burden on forum administrators, who not only need sufficient and up-to-date technical knowledge, but who also have to invest more and more of their time to keep the forum safe and secure.

Additional to the qualitative approach taken in Chapter 2, Chapter 4 also provided insight into the criminal process and evolution of a Darkweb forum, but from a quantitative perspective. The forum studied in Chapter 4 was active for over four years before it was shut down by law enforcement. During the latter 16 months the forum was operational, it transformed from a relatively small, secure and hidden forum into a forum open to new registrations attracting hundreds of new members each month. Under the new forum administrator, various new topic areas were added, leading to a major increase in forum activity. Forum members monthly added between 20,000 and 30,000 posts to the forum. This relates to the notion of forum branding and marketing (found in Chapter 2), which is used to attract new forum members and to develop ‘future-proof’ CSAM communities. It also underlines the need for continuous tutoring of new members about the forum’s safety procedures.

The studies that are part of this dissertation however, also highlight that Darkweb CSAM offending exceeds the criminal realm, and entails more than the sole act of the online exchange of CSAM. Forum members not only discuss the CSAM exchanged on the forum, but forum discussions also include topics such as societal engagement, politics and media. This leads to the conclusion that apart from criminal marketplaces, these illegal Darkweb CSAM fora can also be characterized as social communities.

Online support fora on the Clearnet enabling individuals with a sexual interest in children to engage and communicate with one another through chatrooms, discussion fora and private messaging have been identified as early as 1999 (Durkin & Bryant, 1999). The emergence of peer-to-peer networks could be seen as the first step from CSAM offenders operating primarily individually, towards them committing crimes in online networks in a semi-anonymous setting on a large scale, yet, because of their set-up and infrastructure, the social communication between offenders on these Clearnet peer-to-peer platforms remained limited (Hammond et al., 2009; Hughes et al., 2006; Westlake et al., 2011). O’Halloran and Quayle’s (2010) content analysis of a Clearnet support forum indicates that an important function of such online platforms for individuals is to receive support from like-minded others. Although those observed interacting on these fora are not necessarily CSAM offenders, it does portray the need for marginalized individuals to form communities, where they can safely meet and communicate (see also: Owens et al., 2016; Rimer, 2017). At least

on the Darkweb fora studied here, some forum members appear to not only seek to be part of this community, but also to strive to acquire a higher status in the forum's hierarchy, for example by fulfilling administrative tasks or by uploading original or more extreme material. To fully comprehend CSAM crime, additional to insight into the criminal process of Darkweb CSAM offending, acquiring a more detailed understanding of the non-criminal social processes underlying the forum environment may therefore also be important.

#### 8.1.1.1 Darkweb CSAM does not occur in isolation

The current dissertation further provided evidence that when describing the criminal process of Darkweb CSAM fora, it is important to look further than the forum environment itself. In order for Darkweb CSAM fora to work safely and efficiently, connections to other legal and illegal markets are necessary, for example to gain criminal capital. The suspect interviews and forum communication discussed in Chapter 2 and 3 provided evidence for connections of Darkweb CSAM fora to other Darkweb cybercriminal fora, for example to Darkweb drug markets. CSAM offenders may have a 'sleeping account' on such other cybercriminal fora, used to obtain security advice and techniques. The knowledge obtained on these cybercriminal fora is then used to improve the criminal process and security of the Darkweb CSAM forum.

Moreover, offenders active on Darkweb CSAM fora may also be connected to non-anonymous parts of the internet. Chapter 3 found offenders to have extensive offending histories that originated on the Clearnet. Many Darkweb CSAM offenders had for example been previously active on peer-to-peer networks. Other platforms that were mentioned as a means of accessing CSAM were Google, Skype and Grindr and the Russian website IMGSRU.ru. Furthermore, the case files demonstrated connections to legal pedophilia support websites on the Clearnet. Some offenders also appear to be active on support platforms where the aim is to communicate with peers and where the barter of CSAM is not allowed.

Finally, connections to legal companies and services are pivotal for initiating and maintaining Darkweb CSAM criminal structures. For example, individual members cannot refrain from using legal infrastructures, such as their internet provider and computer operating system, and from using various forms of encryption, data recovery, storage and utility software. The fora itself also need connections to legal platforms in order to operate properly. Firstly, fora need to be hosted on a server. This can either be done by renting storage space with a server provider, or by hosting the server from an offender's home. And a forum needs to be built in a certain format, for which software (for example phpBB) might be used. Legal platforms providing technical support can also be explored by CSAM offenders in order to increase their

knowledge about building and facilitating a forum. Chapter 3 found evidence that administrators and moderators use Clearnet websites to learn about such technical prerequisites to build a forum. Evidence for connections to other Clearnet platforms only indirectly related to the criminal activities, such as hardware-, software-, video editing- and gaming platforms, was also found. The evidence thus suggests that offenders interested in CSAM do not operate in silos, but they will use digital platforms and other technical tools to their convenience.

To conclude, the criminal process of Darkweb CSAM fora clearly extends the forum environment itself. Moreover, the criminal process exceeds individual offending, and can instead be described by large groups of offenders engaged in social communities who increasingly cooperate in an organized way and to whom technical security and support and forum management are essential. The exchange of CSAM on the Darkweb thus does not occur in isolation. This dynamic has resulted in the professionalization and better organization of (Darkweb) CSAM offending. This conclusion directly leads to the second research question: how organized is the crime of CSAM on the Darkweb?

### **8.1.2 How organized is the crime of CSAM on the Darkweb?**

Because of the increasing professionalization and technical sophistication of Darkweb CSAM offending found in Chapter 2, some professionals from law enforcement and academics as well as the media have begun to label Darkweb CSAM offending as organized crime (OC). In order to provide a theoretical exploration of the level and nature of the organization of CSAM on the Darkweb, this dissertation and Chapter 3 more specifically, uses the flexible conception of OC from Von Lampe (2016). When studying criminal processes and phenomena, Von Lampe (2016) argues to reframe the question and ask not whether certain criminal processes are OC or not in a dichotomous way, but rather seek to understand to what extent and in what ways the particular crime is organized. Von Lampe (2016) introduces and distinguishes three types of social structures – entrepreneurial, associational and illegal governance structures – that may influence organized criminal activity. In Chapter 3, six police investigation case files were analyzed using the methodology of the Dutch Organized Crime Monitor (Kruisbergen et al., 2018), accompanied by analyses of interviews with the police officers and public prosecutors involved. The results of this chapter lead to the following description of the organization of Darkweb CSAM offending along the lines of Von Lampe's (2016) three constructs of social structures.

Darkweb CSAM fora can firstly be characterized as digital marketplaces, or entrepreneurial structures, in which illegal goods in the form of CSAM are voluntarily exchanged and where there is overlap between suppliers and demanders. Like for actors in other

criminal markets, there is a risk of exposure by law enforcement, and the need for security leads offenders to screen and get familiar with their co-offenders. In this insecure environment, some level of illegal governance, or enforcement of forum rules and regulations and the resolution of (internal) conflicts, is imposed by forum administrators. In 'business meetings' between forum administrators, decisions about such rules and responses to conflicts are being made. Another important task for forum administrators is to decide about arrangements between forum members served to protect them from threats such as government involvement or other outside attacks to the forum. Darkweb CSAM offending is further embedded in the social network between offenders, or the associational structure, provided by the forum environment (extensively discussed in Chapter 2). The shared sexual interest in children is the social tie that binds forum members, leading to an identification with the community, to unwritten internal social rules of conduct (for example those of politeness and generosity) and to the use of 'slang'. Entrepreneurial structures, illegal governance as well as associational structures can thus clearly be identified within the criminal process of Darkweb CSAM offending.

Additional to the present findings, recent law enforcement reports indicate that the CSAM Darkweb landscape is in continuous movement. It is common for fora to be taken down by law enforcement (Europol, 2016; Europol, 2017; Raven et al., 2021). However, they can also be taken down by administrators for security reasons, for example because of forum members leaking information or illegal material, members compromising the forum, or because of a suspicion of law enforcement intervention. Public information from law enforcement further indicates that fora are expanding, and that they may overlap since members are typically active on various fora throughout time (Europol, 2016; Europol, 2017; Goodman, 2015; Zulkarnine et al., 2016). This means that in the recent past there has been a great number of fora online, with an overlap of forum members, and with members constantly relocating from forum to forum (Boerman et al., 2017; Frank et al., 2010; Goodman, 2015; Westlake et al., 2011; Zulkarnine et al., 2016).

When interpreting this organization and evolution, it can be concluded that Von Lampe's (2016) flexible conception of OC offered new insights into the organization of the criminal process of Darkweb CSAM offending. Although monetary profit, physical violence and the desire to monopolize the market (some traditional characteristics of OC) are largely absent, it can be concluded that the criminal process of Darkweb CSAM offending as well as the offenders involved in it show clear signs of entrepreneurial and social organization. In a criminal landscape that is in continuous movement, cooperation is being established in trust based social networks (further explored in Chapter 7 of this dissertation), overseen by keyplayers who are able to exert some internal governance.

### 8.1.3 Which offender profiles and behavioral patterns can be distinguished on Darkweb CSAM fora?

While initial participation in a Darkweb CSAM forum requires some effort, and on the whole the exchange of CSAM on the forum shows clear signs of organization, this does not mean that every member joining such a forum will become an equally active participant in the online CSAM community. Several typologies of online CSAM offending have been developed (e.g. DeHart et al., 2017; Lanning, 2001; Tener et al., 2015), but so far, no empirical research explicitly examined whether and how CSAM offenders active on the Darkweb fit into those typologies. To answer the research question regarding offender profiles and behavioral patterns on Darkweb CSAM fora, Chapter 4 used a novel methodological approach to analyze forum members' posting behavior derived from criminal career research. Based on a unique dataset consisting of the digital forensic artifacts created by forum members, Chapter 5 examined the behavioral patterns of members who were not communicatively active in the public parts of the forum.

Using all communication data (over 400,000 posts) from four Darkweb CSAM fora and applying Group-Based Trajectory Modeling (GBTM) (Jones & Nagin, 2013; Nagin, 2005), using dimensions such as forum activity onset, posting frequency and posting duration, Chapter 4 distinguished multiple developmental pathways, or trajectories, based on members' posting history. Six trajectories, that can be interpreted as latent offender profiles, were distinguished:

1. The 'lurkers'. The largest group of forum members (58.8% of the sample) shows very little forum activity (a total of 2 posts per member on average). Members allocated to this trajectory enter the forum during its later stages and mostly refrain from posting shortly after entering.
2. The 'browsers'. This group (9.1% of the sample) also typically enters the forum in its later stages and portrays limited posting activity. Still, their average number of posts ( $n = 10.1$ ) is almost five times higher than that of 'lurkers' and also includes posts under the 'Girls hardcore' forum environment category. Additional to their initial registration and application to the forum, it is likely that the majority of members belonging to this group have at least shown some forum browsing (yet non-communicating) activity for a relatively short period of time.
3. The 'CSAM interested'. This group (11.1% of the sample) has an average posting duration of six months and a total of 19 posts (on average) per member. The posting career of this group is more versatile in nature. Over two thirds of the members allocated to this trajectory post under the 'Girls hardcore' environment at least once, while nearly one third post at least once under the 'Boys hardcore' environment.

One in five members allocated to this trajectory also contribute to the 'General discussion' pages of the forum. Over half of the members in this category are registered as 'full member' by the forum administrators, suggesting that they contribute to the forum on a regular basis.

4. The 'escalators'. This group (15.8% of the sample) shows an increase in posting frequency the longer members are active on the forum. Given the timing of their last post, were the forum not taken offline, many members in this trajectory likely would have continued to contribute to the forum. One in ten of the members allocated to this group have a VIP status. As VIP status heavily depends on posting activity, the desire to reach VIP status may partially drive the escalating trajectory.
5. The 'vested members'. Members of this group (4.5% of the sample) first become active already during the early stages of the forum's evolution and have a total of 152 posts (on average) in various sections of the forum. Their posting behavior signals their affinity with the (social) community as a whole. The large majority of members allocated to this group enjoy a 'full member' status, and over one fifth even has a VIP status.
6. The 'managers'. This final group (0.8% of the sample) is characterized by a, compared to members from all other trajectories, high posting frequency ( $n = 1,636$ ). Members of this group do not only post under the 'General discussion' topic; three quarters also post under the 'Information and technical safety' topic, indicating that they are involved in the management of the forum in some way. Members in this group show the longest posting career, and over half of them have an Administrator or VIP status.

Furthermore, from the data it becomes clear that most forum activity takes place in forum environments dedicated to CSAM of girls. That most of the CSAM shared contains illegal images and videos of girls, is also in line with previous research. Insoll et al. (2021) for example found that Darkweb CSAM offenders in their sample most often viewed CSAM related to girls in between the ages of 4 and 13 (45%); compared to 18% who viewed CSAM related to boys in the same age range. Previous studies confirm that most individuals with a sexual interest in children report fantasies about girls. For example, Dombert et al. (2016) report that 68.4% of their sample had an interest in girls, 13.1% in boys and 18.4% in boys as well as girls. Other studies focusing on online CSAM offenders specifically or comparing them to contact offenders, also indicate that a preference for girl victims is the most common (Elliott et al., 2012; Webb et al., 2007). Analyses of law enforcement image databases confirm these results. Interpol for example reports that 65% of the unidentified victims in the International Child Sexual Exploitation Image Database (ICSE), managed by Interpol, are girls (Interpol & ECPAT, 2018).

A study by Quayle and Jones (2011), who examined a sample of CSAM images in a database developed by the Child Exploitation and Online Protection (CEOP) Centre in the United Kingdom, even found that the sample contained four times more girls than boys. Finally, a study in cooperation with the National Center for Missing & Exploited Children (NCMEC) in the United States again confirms that girls are depicted in the majority of CSAM files stored in the NCMEC database (Seto et al., 2018).

From the latent offender profiles, it further becomes evident that a small minority of forum members is responsible for the vast majority of all public forum communication. In other words, a large majority of forum members can be characterized as 'lurkers'. Chapter 5 confirms these results, and finds that on the forum studied in this chapter (which was a different forum than the one studied in Chapter 4) only 3.4% of all forum members showed verbal forum activity. A caveat that needs mentioning however, is that the forum studied in Chapter 5 was an open forum that was considered more as a download platform, and where the risk of being caught was perceived to be high. This may have led to members of this particular forum being less likely to display verbal activity and to expose themselves more than strictly necessary. Despite potential differences in the nature of the fora studied in Chapters 4 and 5, results from both analyses support the notion of a division between highly active keyplayer forum members and far less active general members. Having access not only to the public communication data of a Darkweb CSAM forum, for the study discussed in Chapter 5 the authors also had access to a unique dataset of all members' movements (or clicks) behind the screen/keyboard on the website. Therefore, the behavioral patterns of all forum members, regardless of them being active communicators or not, could be established. As this meant that all forum members, including the 'true lurkers', could be included in the analysis, it was the first time that the behavior of the 'average forum member' could be established. Zooming in on lurking behavior, Chapter 5 finds evidence that the 96.6% of non-communicating members are still behaviorally active on the website. These 'lurking' forum members browse through the website and visit various forum environments.

Furthermore, the analysis in Chapter 5 shows that 93.6% of the forum members, of whom many 'lurking' members, actively download CSAM. On the forum investigated, members download 77 images or videos on average within a period of two weeks. So-called 'lurkers' therefore, although not actively communicating or uploading child abusive content to the forum, do engage with the forum's content in a manner that could encourage others to offend against children and produce new material. By their mere presence on the forum, 'lurkers' create and facilitate the demand and the market for CSAM. This may also mean that 'lurkers' still identify with the forum's predicated interests and experience a sense of belongingness by visiting the forum.

The skewed distributions in online behavior – posting, CSAM sharing as well as downloading – identified in this study corroborate findings from earlier studies examining the downloading and exchange of CSAM on Clearnet peer-to-peer networks, such as Gnutella, BitTorrent, eDonkey and GigaTribe. Wolak and colleagues (2014) for example, who measured a year of online CSAM activity on the Gnutella peer-to-peer network, found that less than 1% of the CSAM users on this peer-to-peer network accounted for a disproportionately high share of CSAM available on the network, each contributing 100 files or more. Over 80% of the CSAM downloaders shared very few CSAM files or were online for only a few days within the year of measurement. Jarlov and colleagues (2009) found similar results on the eDonkey network: most CSAM users contributed only a few files, whereas a very small number of CSAM users provided very large numbers (up to 3,000) of CSAM files (see also: Hughes et al., 2006; Steel, 2009).

To conclude, public opinion greatly condemns those who sexually offend against children. Within this climate, hardly any differentiation between different types of offenders and offenses is being made. The current dissertation adds some nuance to this stance, by establishing various offender profiles and behavioral patterns. Some individuals seem to enter CSAM Darkweb fora out of curiosity rather than out of a fully developed sexual interest in underaged children, which is reflected in their forum activity and behavioral patterns.

#### **8.1.4 How can keyplayers in Darkweb CSAM fora be identified?**

Chapter 6 builds on the notion that keyplayer forum members and general members can be distinguished, and explored alternative ways to automatically identify them from large datasets using various network science methods and techniques (Barabási, 2016).

Network metrics such as various centrality measures enabled to accurately identify keyplayers (such as administrators and moderators) as well as general forum members. The analyses furthermore revealed the more individualistic role of technical keyplayer members dealing with the forum's establishment, encryption and maintenance. It was found that larger forum topics were commented on by less active members, likely because these topics were more easily found and cover a more easily accessible subject. Topics with few comments were commented on by more active members, hinting at an elite of forum members contributing to more specialized (technical) discussions, consisting of keyplayers with roles important to the forum's very existence. Furthermore, the study illuminated the structural properties and distributions of the topics discussed in and members active on the fora. Insights in the forum's anti-lurker and anti-law enforcement policies and new member application guidelines could be deduced only by looking at the network structure of the data. The network data for instance revealed the forum's admission procedure in which members had to provide a post and content in order to gain access to the forum.

The study discussed in Chapter 6 portrayed the added value of multidisciplinary cooperation, with data scientists and criminologists collaborating on the same research problem. Having direct access to expertise within a specialized law enforcement unit, further enabled substantive interpretation of the results and hence, a deeper understanding of the data and the phenomenon under scrutiny. To conclude, distinguishing offender profiles and behavioral patterns (Chapter 4 and 5) and identifying keyplayers (Chapter 6) ultimately aids in the identification of the most active and dangerous Darkweb CSAM offenders, which gives direction to law enforcement's prioritization in CSAM crime investigations.

### **8.1.5 How is trust in Darkweb CSAM fora established?**

Chapter 7 provided a systematic literature review from a criminological as well as psychological perspective linking individual offending motivation and behavior to the aggregation of the CSAM fora using the concept of trust. The reason for focusing on the concept of trust, is that results from Chapter 3 suggested that trust, originating from the associational structures underlying CSAM fora, is important and necessary for two or more offenders to be willing to cooperate (Von Lampe, 2016). Although the concept of trust is not equally important to all forum members, and likely has the greatest value in explaining the behavior of the most active forum members; it is an important concept to comprehend how and why forum members communicate about their deepest sexual feelings online.

Findings from the psychological literature confirm what was also found in the empirical studies of this dissertation: that for some forum members, the engagement in interpersonal communication with like-minded others on Darkweb CSAM fora serves various functions, including justification, normalization, and support, as well as access to expert advice, tutorials and information, and to CSAM itself. Criminological studies highlight that on Darkweb CSAM fora trust initially needs to be established under circumstances of anonymity, without knowing the true identity of one's co-offenders. Information about others and hence their level of trustworthiness is therefore limited. The process of trust establishment may be enhanced by creating a legitimate and reliable online identity. Previous research indicates that members share information about cybercriminal attributes, which then become a personal brand and as such lays the foundation for a reputation that is necessary for trust to be developed further (Lusthaus, 2012; Yip et al., 2013). Trust can be maintained by being visible and portraying oneself as an active member. This includes engaging in frequent online activity, involving posting messages, contributing to open discussions, exchanging valuable advice and by generally being helpful, as well as by mentoring and offering feedback to others. In addition, humor, playfulness, and sarcasm are frequently used to invoke trustworthiness.

To conclude, within the high-stake and high-risk environment of the Darkweb, where members have to manage a continuous flow of threats, such as attacks by hackers or apprehension by law enforcement, the associational structure of the fora lay an important foundation for trust to be established and maintained. It is the commitment and dedication members show to the community which leads to an informal interpretation of a member's forum behavior and to a mutual sense of belonging and trust. This is of social and technical relevance, as it forms the basis for offenders to be willing to cooperate in their criminal endeavors and to proceed in the exchange of CSAM.

## **8.2 Implications of the findings**

To effectively tackle the problem of Darkweb CSAM and to be able to protect victims, it is imperative that strategies and policy are informed by empirical evidence. Up to this point, research specifically focusing on CSAM exchanged on the Darkweb is scarce, because of the Darkweb CSAM fora's illegal nature. Until recently, extant research into CSAM exchanged on other virtual platforms has been dominated by an individual perspective. This means that there is a substantive knowledge base on individual offending and motivation, leading to recommendations about effective therapeutical approaches or law enforcement offender interview strategies. However, there is yet a lot to learn about the structures of online CSAM fora, their hierarchies and role differentiations, and the positions of individual offenders within these fora. As a consequence, there exists a gap in our current knowledge on the cooperation between CSAM offenders, and the overall structure of the larger online CSAM offending landscape. This knowledge is however highly relevant, as it could lead to recommendations about how to strategically fight online CSAM offending, lay bare vulnerable points in the CSAM crime process suitable for intervention, and help identify keyplayer offenders without whom the CSAM forum structures would be greatly disrupted.

By taking an encompassing perspective, the current dissertation contributes to the current academic knowledge by providing detailed insights into the workings of fora where CSAM is exchanged on the Darkweb using multiple disciplinary and methodological perspectives. The criminological, psychological and data science perspective applied in this dissertation complement each other, and lead to the following implications.

### **8.2.1 Implications for law enforcement intervention**

#### **8.2.1.1 Implications from a network perspective**

The first group of implications for law enforcement intervention results from the net-

work perspective taken in this dissertation. Although law enforcement agencies have successfully taken down large CSAM fora in the recent past, and have apprehended some of the keyplayers active on these fora, there are still improvements to be made (Bleakley, 2018; Raven et al., 2021). Historically, CSAM related crime was predominantly committed by individual offenders, and therefore an individual perspective was suitable for law enforcement to tackle this problem. The organized and professional ways in which CSAM related crime is now committed on fora on the Darkweb, asks for revised as well as new law enforcement perspectives.

Law enforcement interventions and techniques suitable to tackle Darkweb CSAM offending have to be intelligence-led (Von Lampe, 2016). Intelligence-led policing involves law enforcement to structurally collect and process information on Darkweb CSAM fora, on its infrastructure, on the individuals active within these fora, and on the nature and severity of the illegal material that is exchanged, for the purposes of intelligence gathering and for making informed decisions about actual criminal investigations. Research repeatedly points out that random attacks on targets in criminal networks are far less effective than informed and targeted ones directed towards keyplayers (Duijn et al., 2014; Frank et al., 2010; Joffres et al., 2011; Westlake et al., 2011; Westlake et al., 2015; Zulkarnine et al., 2016). This finding also applies to Darkweb CSAM fora: the findings of the current dissertation indicate that structurally analyzing these fora and prioritizing those keyplayers with specialized roles within the criminal network for law enforcement intervention, is likely to most effectively disrupt these fora.

More specifically, the organized and professional nature of Darkweb CSAM offending asks for law enforcement to proactively search for those investigations that will likely have the most impact. Wolak and colleagues (2014) for instance, estimated that if law enforcement agencies would arrest the high-contributors on peer-to-peer networks, the number of CSAM files available on the network could be reduced by as much as 30%. An example within the field of Darkweb CSAM offending concerns Darkweb undercover operations aiming to identify the most risky and dangerous keyplayer offenders. When proactively investigating on Darkweb CSAM fora, law enforcement has to deal with large amounts of data to analyze. Single suspects are sometimes responsible for years of communication, leading to datasets comprising of thousands of messages and images to be analyzed. It is not always possible anymore for analysts to physically read through all these data, so therefore advanced and automated analyses are needed (Wolak et al., 2014). This has to involve analysts and data scientists who are capable of conducting sophisticated technical analyses. Looking at the field of Darkweb CSAM from an organized crime perspective, tracking down and focusing on the most important forum members in an intelligence-led manner would professionalize the combat against this type of crime and maximize law enforcement efforts (Westlake et al., 2011).

### 8.2.1.2 Implications from a criminal career perspective

In order to be able to work according to the way proposed, law enforcement has to know the offender group they are dealing with, and the characteristics of the most suitable targets for prioritization (Woodhams et al., 2021). Taking a criminal career perspective, the current dissertation points towards various groups suitable for law enforcement prioritization.

A first obvious group of desirable targets for law enforcement intervention are the administrators and other high-status and highly-active members of Darkweb CSAM fora, who can be seen as forum managers with an active role in facilitating and promoting a social environment in which forum members can exchange CSAM and communicate. While administrators may not always account for a disproportionate share in the exchange of CSAM on their forum, they do play an important role in the establishment and maintenance of the forum. By safeguarding the forum's workings and continuity and by exerting internal governance, administrators and other high-status members are essential in the criminal process and organization. Therefore, a way to disturb a Darkweb CSAM forum is to identify and eliminate the administrators and other keyplayers.

Among this group, the most suitable targets for law enforcement intervention are those 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. Most likely, there will not be dozens of offenders with a sexual interest in children, who also have the technically sophisticated skills to provide this support. Therefore, as the technically sophisticated skills necessary to run a large-scale forum are likely to be reserved to only a minority of CSAM offenders, targeting these offenders is expected to have the greatest impact.

Moreover, not only should law enforcement focus on the current administrators and technical keyplayer members; also the so-called escalators, or potential future keyplayer technical or managerial forum members are worth looking out for, as identifying and arresting them could prevent future crimes from occurring. The current dissertation finds that the group of escalators entails only a small proportion of all Darkweb CSAM forum members, yet their risk for future offending may be significantly elevated, as their online behavior seems to escalate. Escalation in their level of online communication may signal forum members belonging to this group gradually spending more time on the forum, then downloading increasingly severe material, or them increasingly joining conversations about offline abuse. Proactively targeting this offender group before true escalation takes place may be important to prevent future offending, and with that to prevent future victimization of children.

A further offender group suitable for law enforcement intervention, are those forum members active in the very early stages of a forum's existence, regardless of their formal forum status or managerial or technical expertise. These 'vested members' portray behavior that signals their affinity with the community as a whole. Chapter 5 found that the number of members registering during the very early days of a forum's existence is limited and that the number of registered members tends to increase quickly once a forum has been online for some time and becomes known in the wider Darkweb CSAM network. This implies that those members that register in the first week a forum becomes public are potentially interesting targets for law enforcement. Their familiarity with the new forum likely indicates that they have relevant ties to the broader CSAM network, and that they may fulfill a key role in the forum's future development.

Until now, only actively communicating forum members are considered as suitable targets for law enforcement prioritization and intervention. The potential risk of those members that are not active communicators should however not be underestimated. The current dissertation gives evidence that the large majority of forum members, including lurkers, download CSAM and consume the content related to those topics that interest them. It is therefore very likely that lurkers still identify with the forum's predicated interests and even experience a sense of belongingness. Moreover, lurkers on one platform may actually be active participants on other locations and may have important ties with influential fellow forum members or with the larger CSAM network (Cranefield et al., 2015; Tagarelli & Interdonato, 2013). Therefore, there may be value in also detecting lurkers with a high level of forum involvement, indicated by high volumes of (attempted) download- and movement activity (clicks) on the forum. To the extent that downloading CSAM affects attitudes and future behavior, all forum members, including lurkers, may develop toward becoming high-risk offenders, and may become a risk to children in the physical world (Insoll et al., 2021).

It is pivotal to further refine the existing typologies of online CSAM offenders, in order to be able to accurately perform risk assessments to identify the most risky targets on Darkweb CSAM fora. Quantitatively outlining the behaviors of Darkweb CSAM offenders can assist law enforcement in targeting specific fora or specific (groups of) forum members for further (qualitative) assessment and intervention. A more detailed understanding of member profiles and the most risky targets for prioritization is not only useful for the purpose of early detection, but it has further operational advantage when law enforcement professionals are interacting with CSAM offenders online in undercover operations. Studying the language and behavior within online interactions and conversations between prioritized individuals, gives an indication of their social involvement, and may aid in preparing for such operations (Woodhams et al., 2021) and in mirroring offenders' language and behavior to achieve a trusted posi-

tion within the forum (Yip et al., 2013). Law enforcement would benefit from a more established evidence base regarding the type of offender they are dealing with. On a broader level, knowledge resulting from this dissertation as well as related findings could be incorporated in relevant law enforcement training (Woodhams et al., 2021; Martellozzo, 2015).

### **8.2.2 Further implications**

The current dissertation also has implications for professionals other than law enforcement. First of all, as Darkweb CSAM offending is becoming more common (Europol, 2016; Owen & Savage, 2015; Van der Bruggen, 2018; Woodhams et al., 2021), it is only logical that offenders who have been active on the Darkweb will gradually be entering correctional and rehabilitative services. This means that the caseload of forensic psychologists and other practitioners will increasingly consist of Darkweb CSAM offenders (Woodhams et al., 2021). The current dissertation aids these professionals with understanding the Darkweb as an offending platform, not only enabling offenders to collect and exchange CSAM but also providing a social community of like-minded individuals. A more detailed understanding of the different types of offenders active on the Darkweb with varying motivations will help forensic professionals in correctional and rehabilitative services tailoring their services to the type of offender they are dealing with.

This is useful, as different Darkweb forum members may also require different interventions to prevent them from future offending. Previous research has pointed out that treatment levels should be tailored to risk levels (Smid, 2014). As suggested based on the findings in Chapter 4, lower-risk, situationally motivated ‘lurkers’ and ‘browsers’ may be deterred from CSAM offending by increasing their perceived risk of exposure and prosecution. When these offenders are identified and sentenced, for this group low-level treatment for a short period of time or even self-help programs might suffice (Insoll et al., 2021). On the contrary, ‘vested members’ and ‘managers’ – given their vested interests in the CSAM community – likely are not, or to a much lesser extent, deterred from offending simply by an increased risk of exposure and prosecution. For this group, more intensive treatment might be necessary to decrease the likelihood of recidivism. This could be community-based group treatment, or high-intensity mandatory institutional treatment for the highest risk offenders (Smid, 2014; Yang et al., 2021). To conclude, when sufficiently replicated across different samples, typologies such as the ones discussed in this dissertation could be used by clinical forensic professionals and other professionals for specifically assessing Darkweb CSAM offenders for offering them the most effective treatment with the aim of reducing future offending.

Another group of professionals that may learn from the current dissertation are public prosecutors. The results discussed in Chapter 5 provide a summary of the behavior or ‘general profile’ of Darkweb forum members, based on their forum activity, regardless of them being active communicators or not. With these results, prosecutors will be able to assess the behavior of individual offenders, and compare this behavior to the ‘general profile’ of CSAM offenders. For example, prosecutors could exemplify that a certain offender deviates from the general profile regarding the number of visits, clicks, and downloads on a forum, and give an evidence-based judgement of the intensity and severity of an offender’s offending. More specifically, the results may help prosecutors in explaining to the court that despite the suspect showing no verbal activity, this does not necessarily mean that he has not had an active role in facilitating the demand of CSAM by downloading illegal material and thus in the maintenance of the CSAM network as a whole.

Finally, and perhaps most importantly, the current dissertation has implications for prevention. Insoll and colleagues (2021) found that Darkweb CSAM offending often starts at a very young age. Of the Darkweb offenders in their study, 70% had a first time exposure when they were under the age of 18, and 39% was even under the age of 13. Many of them do not appear to be preferential offenders, and their first exposure seems to occur accidentally. For example, they expose themselves because of curiosity, or they have started with viewing legal pornography and have become desensitized. Although the focus of the current dissertation was different – studying offenders active on Darkweb CSAM fora involved with the social aspect of the CSAM community – parallels can still be drawn. The combined results of both studies lead to the hypothesis that the relatively young first-time offenders are most likely part of the category of ‘lurkers’. Although this group may still show offending behavior in terms of browsing through the forum and downloading CSAM, their involvement and grade of activity is significantly lower compared to the groups of more active and dedicated forum members. Therefore, this particular offender group may be susceptible to prevention initiatives, helping them to desist from offending at an early stage, and to not develop into becoming part of the higher-risk groups of ‘escalators’, ‘vested members’ or ‘managers’.

Because of the taboo that rests on sexual offending against children and CSAM, offenders may not very likely seek help from therapists and expose themselves. Therefore, accessible and low-key help is essential. With this in mind, in the Finnish Protect Children Program, the Darkweb survey was accompanied by an online self-help program: an anonymous program for individuals who view and distribute CSAM, based on their thoughts, feelings, and behaviors regarding their use of CSAM, with a goal to maintain behavioral change and stop viewing CSAM (Insoll et al., 2021). Although the

effectiveness of this program has not been tested yet, it is positive that targeted initiatives are being developed and implemented for this particular group of offenders. Other forms of prevention should start even before youngsters become active on the Darkweb, and should involve creating a broader awareness of the problem. As part of the general sexual education of children, they should learn about the risks of the internet and Darkweb for sexual offending, for example from their parents, at school and in treatment facilities (Yang et al., 2021).

## **8.3 Methodological strengths and limitations**

The aim of this dissertation was to explore CSAM fora on the Darkweb using multiple methods. By using various qualitative as well as quantitative methods, new insights about the topic of interest were gained from various angles. As every chapter in this dissertation has its own section discussing the strengths and limitations of the particular method used, this final section only describes the overarching and most important strengths and limitations.

### **8.3.1 Strengths**

The most important strength is that online activities and behavior leave many more traces than do offline activities and behavior, offering a wealth of new data to be studied by academics. This results in knowledge that could not – or at least not as reliably – be obtained without having access to these online data sources. Using Darkweb CSAM forum communication as a data source for this dissertation, enabled to study the hard-to-reach offenders that are scarcely caught by law enforcement. In this regard the current dissertation distinguishes itself from previous studies in this area, that mostly focused on offenders who were prosecuted (e.g. Owens et al., 2016; Shelton et al., 2016), on ex-offenders now receiving treatment (e.g. Seto & Ahmed, 2014), or on offenders active on peer-to-peer networks (e.g. Hughes et al., 2006; Steel, 2009). From a qualitative perspective, research into this hidden offender population through unobtrusive means enables studying the actual and ‘natural’ behavior of these offenders, thereby shedding unique light on concepts such as the criminal process, the criminal organization, offender motivation and trust establishment and maintenance.

From a quantitative perspective, using forum communication and forum member relationships as a data source in this dissertation, enabled to study all forum members active on a Darkweb CSAM forum at once. In this world of big data, with Darkweb CSAM fora sometimes consisting of hundred thousands of members, sophisticated quantitative analyses become a necessary tool to gain insight into the fora’s structures

and to identify the most important forum members. Moreover, using methods like Group-Based Trajectory Modelling or methods from a network or data science perspective, has a number of advantages over content-based analysis of Darkweb forum data, as it only requires derived datasets representing the structure of the forum, and not its actual content. As such, researchers without clearance are also able to analyze these datasets, without committing a crime. Moreover, using derived datasets also allows to analyze encrypted posts and fora in foreign languages. Finally, the dataset studied in Chapter 5 even offered the opportunity to also study the downloading behavior of true lurkers who are not otherwise communicating on the forum. Therefore this study arguably is one of the first – if not the first – studying all forum members on a Darkweb CSAM forum at once.

### 8.3.2 Limitations

Despite their strengths, the studies included in this dissertation also have some limitations. A first set of limitations is related to the generalizability of the results. Though varied in size and structure, the fora used for the current analyses do not constitute a representative sample of all Darkweb CSAM fora in a statistical sense. It is very well possible that there are ‘more inaccessible’ fora online, presently outside the view of law enforcement surveillance. The fora covered in this dissertation are from 2010-2017, and thus relatively old. There have been many more fora online, and likely there will be many more in the future. Although there is no indication that any significant changes in the criminal process, governance structure or member profiles have occurred in recent years; technological developments are likely to result in minor developments and changes on Darkweb CSAM fora. It would therefore be sensible to replicate the current studies and develop new studies on more recent Darkweb CSAM fora. When not having access to the data through cooperation with a law enforcement agency, Darkweb crawling and classification methods developed by academics may aid in reliably analyzing more recent data (Dalins et al., 2018). Finally, in terms of generalizability, the findings in this dissertation likely do not apply to all individuals interested in CSAM, as the dissertation specifically zooms in on the group of offenders active on CSAM fora on the Darkweb. Although the ratio of offenders active on the Darkweb versus the offenders active on the Clearnet is not known, interviews and informal conversations with law enforcement personnel pointed out that, for example because of its speed compared to the Darkweb, the Clearnet is still often used by CSAM offenders.

The illegal nature of the material discussed and exchanged on CSAM fora on the Darkweb introduces another hurdle in the scientific analysis of these online communities. Due to its illegal nature, only researchers with special clearance are able to conduct these analyses – which in case of the studies included in this dissertation meant

that much of the data was reviewed and coded by the first author only, who, at the time of writing, was a sworn-in police officer at the National Police of the Netherlands. Only data relating to the frequency, timing, and structural dimensions of forum members' online communications could be shared with others involved in the project. This introduces the risk of single rater bias, especially when qualitatively analyzing the forum data. To mitigate this risk, during all stages of analysis, the coding and findings were discussed with specialized police personnel involved in the police investigations where the data originated from, such to safeguard correct interpretation of the fora's workings and the nature of the data gathered.

Moreover, although innovative, there are some limitations more specific to studies using Darkweb communication data. More specifically, some potential crucial data was excluded from the current studies. The data available only covered forum communication posted on the public areas of the fora. Therefore, there was no way of estimating the size and nature of the private communication going on between members. Because of its even more private nature, this communication will most likely contain the most sensitive topics, potentially discussed in more detail. Moreover, although general estimates of the type of CSAM exchanged on the various Darkweb fora under investigation were conducted, this dissertation did not include an assessment of the actual CSAM exchanged or collected through the fora and it did not use the material exchanged as unit of analysis.

These limitations touch on a larger debate. Although online activities and behavior leave many traces, and the accessibility of online data continues to grow, the possibilities to make this data available to researchers are still scant. This relates to challenges in making datasets containing material of an illegal nature available to researchers in a non-sensitive or derived way to allow them to study these data, as well as in challenges related to transform the often very large online datasets in analyzable formats. Most research projects in this area, including all studies included in this dissertation, therefore rely on intensive cooperation with law enforcement personnel who have access to the data and the clearance to view the actual material. The current research would simply have been impossible if such intensive cooperation could not be obtained. This observation leads to some suggestions for future research directions.

## **8.4 Future research directions**

There are other and newer ways in which sensitive and illegal data, such as the data studied in this dissertation, could be made available to researchers. To learn about the organizational structures of Darkweb CSAM fora, research methods using these fora's

meta-data, may be of help here. Moreover, various researchers have begun to use technical tools that automatically make images and videos inaccessible, which eliminates the illegal forum content but leaves the structure of the forum intact for researchers to analyze without them being liable to prosecution (e.g. Web-1Q, 2018). Connecting hashes, or digital footprints, to the images and videos, would even enable researchers to describe the nature and severity of these images without having to be exposed to them. Working in this manner would not only solve the single coder bias resulting from the sensitive and illegal nature of the data specific to the current dissertation discussed in Chapter 2, but in a much broader way it would make data available and analyzable to many more researchers. Working in this way enables a number of quantitative research avenues to be explored further.

The Darkweb CSAM forum's underlying communication network, its structure, strengths, and weaknesses can be studied using mathematical concepts and techniques from the social network analysis (Morselli & Roy, 2008; Tompson & Chainey, 2011). Identifying keyplayers and brokerage positions, and seeking ways to optimally disrupt these fora so to prevent them from victimizing children remains an important topic of future study (Westlake et al., 2011). Taking a criminal career perspective, future research could assess the extent to which it is possible to predict members' future forum position, based on the development of their online communications. In this way, interventions could be aimed at curbing members' developmental pathway, preventing their online offending from spiraling out of control and them attaining central positions in the CSAM forum.

Moreover, the current dissertation points toward two types of data that could be included in future academic research. First, the most sensitive conversations will most likely occur in private messaging, therefore future network studies could compare the results of this dissertation with analyses conducted on these private messages. Secondly, the results of Chapter 5 imply that (attempts to) downloading CSAM is the main reason for many members to visit Darkweb CSAM fora. In order to explore downloading behavior in more detail, future studies should include the meta-data of the images themselves in their datasets.

Following another methodology, members' online behaviors can also be further explored by simply asking forum members about it. The study by Insoll and colleagues (2021) contained a first attempt of doing so. At the time of writing this conclusion, the survey developed by Insoll and colleagues (2021) was still accessible on the Darkweb, and had already received over 10,000 responses. Surveys such as these give novel and detailed insights originating directly from the offenders themselves, who remain anonymous and are as yet unknown to law enforcement, let alone to academics. The continuation of such studies is paramount to understand the CSAM landscape in all its breadth.

Finally, Darkweb offender communication also offers vast datasets to be further explored qualitatively. Following Chapter 7 of this dissertation, the process through which individuals seek to establish trust and develop relationships with other members on Darkweb CSAM fora could be examined in more depth when qualitatively studying the language of public and private messages exchanged by forum members. From this communication, researchers could for example deduce which aspects and features forum members take into consideration when making the decision of whether or not another member is trustworthy enough to initiate contact and develop a relationship with. In addition, it would be useful to explore in more detail how trust-based personal relationships between co-offenders may trigger the formation of smaller sub-networks, and how this may contribute to the progression and escalation of offending behavior. Besides trust, other relevant concepts to be explored qualitatively include behavioral differences between keyplayer and general forum members, factors that lead offenders to start communicating on a forum and rise in the forum's hierarchy, offending methods, techniques and cooperation, and the establishment of either friendship or competition. More generally, more in-depth analysis is needed to gain deeper insight into the thoughts, feelings, and behaviors of Darkweb CSAM offenders to protect children from future crimes (Insoll et al., 2021).

#### **8.4.1 Bridging the gap between law enforcement and science**

The current dissertation is one of the first exploring CSAM fora on the Darkweb. Only recently, research papers on this topic have started to emerge (e.g. Insoll et al., 2021, Kokolaki et al., 2020, Woodhams et al., 2021, Yang et al., 2021). In other words, the research in this area is still young. One of the explanations for this is the fact that this type of research needs in-depth knowledge about law enforcement and the offender community as well as knowledge about science and scientific research methods. This means that an open-minded and optimistic cooperation between law enforcement communities and academic communities needs to be continued and further developed (Baechler, 2019; Duijn & Klerks, 2014; Jarlov et al., 2009). Despite the growing number of instances in which such intensive collaboration is indeed achieved, some obstacles preventing cooperation also need mentioning. One important obstacle is the different pace of law enforcement and that of academic activities. Where policing is characterized by 'fast thinking' and often occurs in real time, academic thinking is often slow and prepares for the medium to long term (Baechler, 2019; Kahneman, 2011). Furthermore, law enforcement often expresses a need for concrete answers to specific cases or specific questions and for policies that can be implemented directly. Academic research on the contrary, is often focused on scientific problem-solving and draws conclusions about generalities that might not directly answer the concrete questions put forth by

law enforcement. This may result in difficulties in understanding each other's context and objectives (Baechler, 2019; Telep, 2017), which in its turn may obstruct a trustful and fruitful relationship in which possibilities to share knowledge and data within the boundaries of the law are continuously explored.

Striving for effective intelligence-led and evidence-based policing (Von Lampe, 2016), strong and fruitful relationships between law enforcement and academics can be built or maintained by the means of for example shared PhD-professional positions, mutual and continuous education and training courses, collaborative student projects, or community-building initiatives (Baechler, 2019). Working closely together in this regard will help smooth the translation and implementation of academic findings into practically applicable recommendations for professional practice. Moreover, the issues of confidentiality, privacy, and security when it comes to data-sharing from a governmental and law enforcement perspective can be more easily overcome.

Because of the public demand for such material, CSAM is – however unfortunate this may be – strongly embedded in our present day society (Von Lampe, 2016). The internet, and with it online (Darkweb) CSAM fora, has developed very rapidly and CSAM offenders continuously traverse to newer platforms in increasing anonymity. It is therefore essential that academic research stays up to date with the latest technological developments, and has the courage to explore new areas and platforms of research. The expertise, knowledge and input from law enforcement in this regard is pivotal. Intensive collaboration between researchers from different disciplines, and between academic, law enforcement, and private partners is therefore our best chance of effectively protecting children in the future.





# REFERENCES

- Aaltonen, M. (2021). *Using the findings of research on CSAM users to strengthen global child protection efforts. What have we learnt and where do we go from here?* [Conference presentation]. ReDirection International Expert Webinar.
- Afroz, S., Garg, V., McCoy, D., & Greenstadt, R. (2013). Honor among thieves: A common's analysis of cybercrime economies. *APWG eCrime Researchers Summit*, 1-11. <https://doi.org/10.1109/eCRS.2013.6805778>
- Alharbi, A., Faizan, M., Alosaimi, W., Alyami, H., Agrawal, A., Kumar, R., & Ahmad Khan, R. (2021). Exploring the topological properties of the tor dark web. *IEEE Access*, 9, 21746–21758. <https://doi.org/10.1109/ACCESS.2021.3055532>
- Babchishin, K.M., Hanson, R.K. & VanZuylen, H. (2015). Online child pornography offenders are different: A meta-analysis of the characteristics of online and offline sex offenders against children. *Archives of Sexual Behavior*, 44, 45–66. <https://doi.org/10.1007/s10508-014-0270-x>
- Baechler, S. (2019). Do we need to know each other? Bridging the gap between the university and the professional field. *A Journal of Policy and Practice*, 13(1), 102–114. <https://doi.org/10.1093/police/pax091>
- Bakken, S.A., Moeller, K., & Sandberg, S. (2017). Coordination problems in crypto-markets: Changes in cooperation, competition and valuation. *European Journal of Criminology*, 15(4), 1-19. <https://doi.org/10.1177/1477370817749177>
- Balfe, M., Gallagher, B., Masson, H., Balfe, S., Brugha, R., & Hackett, S. (2015). Internet child sex offenders' concerns about online security and their use of identity protection technologies: A review. *Child Abuse Review*, 24(6), 427–439. <https://doi.org/10.1002/car.2308>
- Barabási, A.L. (2016). *Network Science*. Cambridge University Press.
- Bartlett, J. (2014). *The Dark Net: Inside the digital underworld*. Maven Publishing.
- Beauregard, E., & Leclerc, B. (2007). An application of the rational choice approach to the offending process of sex offenders: A closer look at the decision-making. *Sexual Abuse*, 19(2), 115–133. <https://doi.org/10.1177/107906320701900204>
- Beauregard, E., Proulx, J., Rossmo, K., Leclerc, B., & Allaire, J. (2007). Script analysis of the hunting process of serial sex offenders. *Criminal Justice and Behavior*, 34(8), 1069–1084. <https://doi.org/10.1177/0093854807300851>
- Beckert, J., & Wehinger, F. (2013). In the shadow: Illegal markets and economic sociology. *Socio-Economic Review*, 11(1), 5-30. <https://doi.org/10.1093/ser/mws020>

- Beech, A.R., Elliott, I.A., Birgden, A., & Findlater, D. (2008). The internet and child sexual offending: A criminological review. *Aggression and Violent Behavior*, 13, 216–228. <https://doi.org/10.1016/j.avb.2008.03.007>
- Best, J., & Luckenbill, D.F. (1980). The social organization of deviants. *Social Problems*, 28(1), 14–31. <https://doi.org/10.2307/800378>
- Bleakley, P. (2018). Watching the watchers: Taskforce Argos and the evidentiary issues involved with infiltrating Dark Web child exploitation networks. *The Police Journal: Theory, Practice, Principles*, 92(3), 221–236. <https://doi.org/10.1177/0032258X18801409>
- Blokland, A. (2018). Taking a criminal career approach to sexual offending. In P. Lussier & E. Beauregard (Eds.), *Sexual offending: A criminological perspective* (1<sup>st</sup> ed., pp. 141–155). Routledge.
- Blokland, A., & Lussier, P. (2015). *Sex offenders: A criminal career approach*. Wiley-Blackwell.
- Blumstein, A., Cohen, J., & Farrington, D.P. (1988). Longitudinal and criminal career research: Further clarifications. *Criminology*, 26(1), 57–74. <http://www.ncjrs.gov/App/publications/abstract.aspx?ID=110130>
- Boerman, F., Grapendaal, M., Nieuwenhuis, F., & Stoffers, E. (2017). *Nationaal Dreigingsbeeld 2017: georganiseerde criminaliteit*. Dienst Landelijke Informatieorganisatie (Politie).
- Bonachich, P. (1987). Power and centrality: A family of measures. *American Journal of Sociology*, 92(5), 1170–1182.
- Borgatti, S.P. (2006). Identifying sets of key players in a social network. *Computational & Mathematical Organization Theory*, 12(1), 21–34. <https://doi.org/10.1007/s10588-006-7084-x>
- Borrior, H. (2013). Quality assurance in crime scripting. *Crime Science*, 2(6). <https://doi.org/10.1186/2193-7680-2-6>
- Bozkurt, A., Koutropoulos, A., Singh, L., & Honeychurch, S. (2020). On lurking: Multiple perspectives on lurking within an educational community. *The Internet and Higher Education*, 44. <https://doi.org/10.1016/j.iheduc.2019.100709>
- Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), 77–101. <http://doi.org/10.1191/1478088706qp0630a>
- Brayley, H., Cockbain, E., & Laycock, G. (2011). The value of crime scripting: Deconstructing internal child sex trafficking. *A Journal of Policy and Practice*, 5, 132–143. <https://doi.org/10.1093/police/par024>
- Brennan, M., & Hammond, S. (2017). A methodology for profiling paraphilic interest in child sexual exploitation material users on peer-to-peer networks. *Journal of Sexual Aggression*, 23(1), 90–103. <https://doi.org/10.1080/13552600.2016.1241308>

- Brin, S., & Page, L. (1998). The anatomy of a large-scale hypertextual web search engine. *Computer Networks and ISDN Systems*, 30(1-7), 107-117. [https://doi.org/10.1016/S0169-7552\(98\)00110-X](https://doi.org/10.1016/S0169-7552(98)00110-X)
- Broadhurst, R., Grabosky, P., Alazab, M., Bouhours, B., & Chon, S. (2014). Organizations and cyber crime: An analysis of the nature of groups engaged in cyber crime. *International Journal of Cyber Criminology*, 8(1), 1-20. <https://ssrn.com/abstract=2461983>
- Broome, L.J., Izura, C., & Davies, J. (2020). A psycho-linguistic profile of online grooming conversations: A comparative study of prison and police staff considerations. *Child Abuse & Neglect*, 109. <https://doi.org/10.1016/j.chiabu.2020.104647>
- Caldwell, M.F. (2016). Quantifying the decline in juvenile sexual recidivism rates. *Psychology, Public Policy, and Law*, 22(4), 414 - 426. <http://dx.doi.org/10.1037/law0000094>
- Canadian Centre for Child Protection (2017). *Survivors' Survey: Executive Summary 2017*. CCCP. [www.protectchildren.ca/pdfs/C3P\\_SurvivorsSurveyExecutiveSummary2017\\_en.pdf](http://www.protectchildren.ca/pdfs/C3P_SurvivorsSurveyExecutiveSummary2017_en.pdf)
- Canadian Centre for Child Protection. (2018). *Protect we will* (Social value report 2016-2017). [https://www.protectchildren.ca/pdfs/C3P\\_SocialValueReport\\_2016-2017\\_en.pdf](https://www.protectchildren.ca/pdfs/C3P_SocialValueReport_2016-2017_en.pdf)
- Caneppele, S., & Aebi, M. (2019). Crime drop or police recording flop? On the relationship between the decrease of offline crime and the increase of online and hybrid crimes. *Policing: A Journal of Policy and Practice*, 13(1), 66-79. <https://doi.org/10.1093/polic/pax055>
- Carnes, P.J. (2003). The anatomy of arousal: Three internet portals. *Sexual and Relationship Therapy*, 18(3), 309-328. <https://doi.org/10.1080/14681990310153937>
- Chiang, E., & Grant, T. (2019). Deceptive identity performance: Offender moves and multiple identities in online child abuse conversations. *Applied Linguistics*, 40(4), 675-698. <https://doi.org/10.1093/applin/amy007>
- Chiu, Y., & Leclerc, B. (2017). An examination of sexual offenses against women by acquaintances: The utility of a script framework for prevention purposes. In B. Leclerc & E. Savona (Eds.), *Crime prevention in the 21<sup>st</sup> century* (1<sup>st</sup> ed., pp. 59-76). Springer.
- Chiu, Y., Leclerc, B., & Townsley, M. (2011). Crime Script Analysis of drug manufacturing in clandestine laboratories: Implications for prevention. *The British Journal of Criminology*, 51(2), 355-374. <https://doi.org/10.1093/bjc/azr005>
- Cohen-Almagor, R. (2013). Online child sex offenders: Challenges and counter-measures. *The Howard Journal of Criminal Justice*, 52(2), 190-215. <https://doi.org/10.1111/hojo.12006>
- Cooper, A. (1998). Sexuality and the internet: Surfing into the new millennium. *CyberPsychology and Behavior*, 1, 187-193. <https://www.liebertpub.com/doi/10.1089/cpb.1998.1.187>

- Cornish, D. (1994). The procedural analysis of offending and its relevance for situational prevention. In R. Clarke (Ed.), *Crime prevention studies* (Vol. 3, pp. 151–196). Criminal Justice Press.
- Cornish, D., & Clarke, R. (2002). Analyzing organized crimes. In A.R. Piquero & S.G. Tibbets (Eds.), *Rational choice and criminal behavior: Recent research and future challenges* (1<sup>st</sup> ed., pp. 41–64). Routledge.
- Cranefield, J., Yoong, P., & Huff, S. (2015). Rethinking lurking: Invisible leading and following in a knowledge transfer ecosystem. *Journal of the Association for Information Systems*, 16(4), 213–247. <https://doi.org/10.17705/ijais.00394>
- Cross, J.C. (2000). Passing the buck: Risk avoidance and risk management in the illegal/informal drug trade. *International Journal of Sociology and Social Policy*, 20(9–10), 68–94. <https://doi.org/10.1108/01443330010789232>
- Dalins, J., Wilson, C., & Carman, M. (2018). Criminal motivation on the dark web: A categorisation model for law enforcement. *Digital Investigation*, 24, 62–71. <https://doi.org/10.1016/j.diin.2017.12.003>
- Davis, R.A. (2001). A cognitive-behavioral model of pathological internet use. *Computers in Human Behavior*, 17(2), 187–195. [https://doi.org/10.1016/S0747-5632\(00\)00041-8](https://doi.org/10.1016/S0747-5632(00)00041-8)
- Décary-Héty, D., & Dupont, B. (2013). Reputation in a dark network of online criminals. *Global Crime*, 14(2–3), 175–196. <https://doi.org/10.1080/17440572.2013.801015>
- DeHart, D., Dwyer, G., Seto, M.C., Moran, R., Letourneau, E., & Schwarz-Watts, D. (2017). Internet sexual solicitation of children: A proposed typology of offenders based on their chats, e-mails, and social network posts. *Journal of Sexual Aggression*, 23(1), 77–89. <https://doi.org/10.1080/13552600.2016.1241309>
- Dehghanniri, H., & Borrión, H. (2019). Crime scripting: A systematic review. *European Journal of Criminology*, 18(4), 504–525. <https://doi.org/10.1177/1477370819850943>
- DeMarco, J., Sharrock, J., Crowther, T., & Barnard, M. (2018). *Behaviour and characteristics of perpetrators of online-facilitated child sexual abuse and exploitation: A rapid evidence assessment*. Independent Inquiry into Child Sexual Abuse.
- Dombert, B., Schmidt, A., Banse, R., Briken, P., Hoyer, J., Neutze, J., & Osterheider, M. (2016). How common is men's self-reported sexual interest in prepubescent children?, *The Journal of Sex Research*, 53(2), 214–223. <https://doi.org/10.1080/00224499.2015.1020108>
- Duijn, P. (2016). *Detecting and disrupting criminal networks: a data driven approach*. [Dissertation, University of Amsterdam].
- Duijn, P., Kashirin, V., & Sloot, P. (2014). The relative ineffectiveness of criminal network disruption. *Scientific Reports*, 4, 1–15. <https://doi.org/10.1038/srep04238>
- Duijn, P., & Klerks, P. (2014). De brug tussen wetenschap en opsporingspraktijk: Onderzoek naar de toepassing van sociale netwerkanalyse in de opsporing. *Tijdschrift voor Criminologie*, 56(4), 39–70. <https://doi.org/10.5553/TvC/0165182X2014056004003>

- Dupont, B. (2013). Skills and trust: a tour inside the hard drives of computer hackers. In C. Morselli (Ed.), *Illicit networks* (pp. 195-217). Routledge.
- Dupont, B., Côté, A., Boutin, J., & Fernandez, J. (2017). Darkode: Recruitment patterns and transactional features of “the most dangerous cybercrime forum in the world”. *American Behavioral Scientist*, 61(11), 1219-1243. <https://doi.org/10.1177/0002764217734263>
- Dupont, B., Côté, A., Savine, C., & Décary-Héту, D. (2016). The ecology of trust among hackers. *Global Crime*, 17(2), 129-151. <https://doi.org/10.1080/17440572.2016.1157480>
- Durkin, K.F., & Bryant, C.D. (1999). Propagandizing pederasty: A thematic analysis of the on-line exculpatory accounts of unrepentant pedophiles. *Deviant Behaviour: An Inter-Disciplinary Journal*, 20, 103-127. <https://doi.org/10.1080/016396299266524>
- Durkin, K.F., Forsyth, C.J., & Quinn, J. F. (2006). Pathological internet communities: A new direction for sexual deviance research in a post modern era. *Sociological Spectrum*, 26(6), 595-606. <https://doi.org/10.1080/02732170600948857>
- Duwe, G. (2014). To what extent does civil commitment reduce sexual recidivism? Estimating the selective incapacitation effects in Minnesota. *Journal of Criminal Justice*, 42(2), 193-202. <https://doi.org/10.1016/j.jcrimjus.2013.06.009>
- Eck, J.E. (1995). A general model of the geography of illicit retail marketplaces. In J. Eck & D. Weisburd (Ed.), *Crime and place: Crime prevention studies* (4<sup>th</sup> ed., pp. 67-93). Criminal Justice Press.
- Egan, M. (2018). *Thinking of venturing on to the dark web? You might want to change your mind*. Tech Advisor. <https://www.techadvisor.co.uk/how-to/internet/dark-web-3593569/>
- Elliott, I.A., & Beech, A.R. (2009). Understanding online child pornography use: Applying sexual offense theory to internet offenders. *Aggression and Violent Behavior*, 14(3), 180-193. <https://doi.org/10.1016/j.avb.2009.03.002>
- Elliott, I.A., Beech, A.R., & Mandeville-Norden, R. (2013). The psychological profiles of internet, contact, and mixed internet/contact sex offenders. *Sexual Abuse*, 25(1), 3-20. <https://doi.org/10.1177/1079063212439426>
- Europol (2016). *Internet Organised Crime Threat Assessment (iOCTA)*. Europol.
- Europol (2017). *Internet Organised Crime Threat Assessment (iOCTA)*. Europol.
- Europol (2018). *Internet Organised Crime Threat Assessment (iOCTA)*. Europol.
- Europol (2019). *Internet Organised Crime Threat Assessment (iOCTA)*. Europol.
- Europol (2020). *Exploiting isolation: Offenders and victims of online child sexual abuse during the Covid-19 pandemic*. Europol.
- Felson, M. (2003). The process of co-offending. In M.J. Smith & D.B. Cornish (Eds.), *Theory for practice in situational crime prevention* (pp. 149-168). Willan Publishing.

- Felson, M. (2006). *The ecosystem for organized crime*. HEUNI.
- Finklea, K. (2017). *Darkweb*. Congressional Research Service. <https://fas.org/sgp/crs/misc/R44101.pdf>
- Fonhof, A., Van der Bruggen, M., & Takes, F. (2018). Characterizing key players in child exploitation networks on the Dark Net. *Complex Networks*, 813, 412–423. [https://doi.org/10.1007/978-3-030-05414-4\\_33](https://doi.org/10.1007/978-3-030-05414-4_33)
- Fortin, F., & Proulx, J. (2019). Sexual interests of child sexual exploitation material (CSEM) consumers: Four patterns of severity over time. *International Journal of Offender Therapy and Comparative Criminology*, 63(1), 55–67. <https://doi.org/10.1177/0306624X18794135>
- Frank, R., Westlake, B., & Bouchard, M. (2010). The structure and content of online child exploitation networks. *Workshop on intelligence and security informatics* (pp. 1–9). <https://dl.acm.org/doi/10.1145/1938606.1938609>
- Ghosh, S., Das, A., Porras, P., Yegneswaran, V., & Gehani, A. (2017). Automated categorization of onion sites for analyzing the Darkweb ecosystem. *Proceedings of the 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*. 1793–1802. <https://doi.org/10.1145/3097983.3098193>
- Gibson, L., Linden, R., & Johnson, S. (1980). A situational theory of rape. *Canadian Journal of Criminology*, 22, 51–65. <http://www.ncjrs.gov/App/publications/abstract.aspx?ID=65103>
- Gilmour, N. (2014). Understanding money laundering: A crime script approach. *The European Review of Organised crime*, 1(2), 35–56. <https://doi.org/10.1016/j.ijl-cj.2015.03.002>
- Goldsmith, J. & Wu, T. (2006). *Who controls the Internet? Illusions of a borderless world*. Oxford University Press.
- Gong, W., Lim, E., & Zhu, F. (2015). Characterizing silent users in social media communities. *Proceedings of the Ninth International AAAI Conference on Web and Social Media*, 140–149. [https://ink.library.smu.edu.sg/sis\\_research/3107](https://ink.library.smu.edu.sg/sis_research/3107)
- Goodman, M. (2015). *Future Crimes: Inside the digital underground and the battle for our connected world*. Transworld Publishers.
- Grady, M.D., Levenson, J. S., Mesias, G., Kavanagh, S., & Charles, J. (2019). “I can’t talk about that”: Stigma and fear as barriers to preventive services for minor-attracted persons. *Stigma and Health*, 4(4), 400–410. <https://doi.org/10.1037/sah0000154>
- Greenberg, D.F. (2014). Studying New York City’s crime decline: Methodological issues. *Justice Quarterly*, 31(1), 154–188. <https://doi.org/10.1080/07418825.2012.752026>
- Griffiths, G., & Norris, G. (2020). Explaining the crime drop: Contributions to declining crime rates from youth cohorts since 2005. *Crime, Law and Social Change*, 73, 25–53. <https://doi.org/10.1007/s10611-019-09846-5>

- Hammond, S., Quayle, E., Kirakowski, J., O'Halloran, E., & Wynne, F. (2009). *An examination of problematic paraphilic use of Peer to Peer facilities*. MAPAP Project. <http://antipaedo.lip6.fr/T24/TR/hebe.pdf>
- Hanson, R.K., Harris, A.J.R., Letourneau, E., Helmus, L.M., & Thornton, D. (2018). Reductions in risk based on time offense-free in the community: Once a sexual offender, not always a sexual offender. *Psychology, Public Policy, and Law*, 24(1), 48-63. <https://doi.org/10.1037/law0000135>
- Hobbs, D. (2013). *Lush life: Constructing organized crime in the UK*. Oxford University Press.
- Holt, T.J. (2010). Exploring strategies for qualitative criminological and criminal justice inquiry using on-line data. *Journal of Criminal Justice Education*, 21(4), 466-487. <https://doi.org/10.1080/10511253.2010.516565>
- Holt, T. (2010). Examining the role of technology in the formation of deviant subcultures. *Social Science Computer Review*, 28(4), 466-481. <https://doi.org/10.1177/0894439309351344>
- Holt, T. (2012). Examining forces shaping cybercrime markets online. *Social Science Computer Review*, 31(2), 165-177. <https://doi.org/10.1177/0894439312452998>
- Holt, T., Blevins, K., Burkert, N. (2010). Considering the pedophile subculture online. *Sexual Abuse: A Journal of Research and Treatment*, 22(1), 3-24. <https://doi.org/10.1177/1079063209344979>
- Holt, T., Blevins, K.R., & Kuhns, J.B. (2014). Examining diffusion and arrest avoidance practices among Johns. *Crime & Delinquency*, 60(2), 261-283. <https://doi.org/10.1177/0011128709347087>
- Holt, T.J., & Bossler, A.M. (2014). An assessment of the current state of cybercrime scholarship. *Deviant Behavior*, 35(1), 20-40. <https://doi.org/10.1080/01639625.2013.822209>
- Holt, T., Smirnova, O., Chua, Y.T., & Copes, H. (2015). Examining the risk reduction strategies of actors in online criminal markets. *Global Crime*, 16(2), 81-103. <https://doi.org/10.1080/17440572.2015.1013211>
- Hout, M.C. van, & Bingham, T. (2013). Surfing the Silk Road: A study of users' experiences. *International Journal of Drug Policy*, 24(6), 524-529. <https://doi.org/10.1016/j.drugpo.2013.08.011>
- Hout, M.C. van, & Bingham, T. (2014). Responsible vendors, intelligent consumers: Silk Road, the online revolution in drug trading. *International Journal of Drug Policy*, 25(2), 183-189. <https://doi.org/10.1016/j.drugpo.2013.10.009>
- Hsu, M., Chang, C., & Yen, C. (2011). Exploring the antecedents of trust in virtual communities. *Behaviour & Information Technology*, 30(5), 587-601. <https://doi.org/10.1080/0144929X.2010.549513>

- Hughes, D., Walkerdine, J., Coulson, G., & Gibson, S. (2006). Is deviant behavior the norm on P2P file-sharing networks? *IEEE Distributed Systems Online*, 7(2). <https://doi.org/10.1109/MDSO.2006.13>
- Huikuri, S. (2021). *Dark Web chatlogs and offender conversations* [Conference presentation]. ReDirection International Expert Webinar.
- Hutchings, A., & Holt, T.J. (2015). A crime script analysis of the online stolen data market. *British Journal of Criminology*, 55(3), 596–614. <https://doi.org/10.1093/bjc/azu106>
- Hutchings, A., & Holt, T.J. (2017). The online stolen data market: Disruption and intervention approaches. *Global Crime*, 18(1), 11–30. <https://doi.org/10.1080/17440572.2016.1197123>
- ICMEC (2018). *Child sexual abuse material: Model legislation & global review*. International Centre for Missing and Exploited Children.
- Insoll, T., Ovaska, A., & Vaaranen-Valkonen, N. (2021). *CSAM users in the Dark Web: Protecting children through prevention*. Suojellaan Lapsia ry. / Protect Children.
- Interagency Working Group (2016). *Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse*. EPCAT International.
- Interpol & ECPAT (2018). *Towards a global indicator on unidentified victims in child sexual exploitation material: Technical report*. Interpol & ECPAT International.
- Jacobs, B. (1993). Undercover deception clues: A case of restrictive deterrence. *Criminology*, 31(2), 281–299. <https://doi.org/10.1111/j.1745-9125.1993.tb01131.x>
- Jacobs, B. (1999). *Dealing crack: The social world of street corner selling*. Northeastern University Press.
- Jardine, E. (2015). *The Dark Web dilemma: Tor, anonymity and online policing*. Global Commission on Internet Governance. [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2667711](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2667711)
- Jarlov, P., Latapy, M., Aidouni, F., Magnien, C., Berger, C., & Crispino, F. (2009). *Monitoring pedophile activity in a P2P network*. MAPAP Project. <http://antipaedo.lip6.fr/results.htm>
- Jenkins, P. (2001). *Beyond Tolerance: Child pornography on the internet*. New York University Press.
- Jenkins, R.E., & Thomas, A.R. (2004). *Deviance online: Portrayals of bestiality on the internet*. Center for Social Science Research.
- Jin, X., Lee, M., & Cheung, C. (2010). Predicting continuance in online communities: Model development and empirical test. *Behaviour & Information Technology*, 29(4), 383–394. <https://doi.org/10.1080/01449290903398190>
- Joffres, K., Bouchard, M., Frank, R., & Westlake, B. (2011). Strategies to disrupt online child pornography networks. *European Intelligence and Security Informatics Conference*, 163–170. <https://doi.org/10.1109/EISIC.2011.32>

- Johnson, B. & Natarajan, M. (1995). Strategies to avoid arrest: Crack sellers' response to intensified policing. *American Journal of Police*, 14(3-4), 49-69. <https://doi.org/10.1108/07358549510111947>
- Jones, B., & Nagin, D. (2013). A note on a Stata plugin for estimating group based trajectory models. *Sociological Methods and Research*, 42(4), 608-613. <https://doi.org/10.1177/0049124113503141>
- Kahneman, D. (2011). *Thinking Fast and Slow*. Allen Lane.
- Kaur, S., & Randhawa, S. (2020). Dark Web: A web of crimes. *Wireless Personal Communications*, 112, <https://doi.org/10.1007/s11277-020-07143-2>
- Kim, J., Bushway, S., & Tsao, H-S. (2015). Identifying classes of explanations for crime drop: Period and cohort effects for New York State. *Journal of Quantitative Criminology*, 32(3), 357-375. <https://doi.org/10.1007/s10940-015-9274-5>
- Kinzel, A. (2021). *The language of online child sexual groomers: A corpus assisted discourse study of intentions, requests and grooming duration*. [Doctoral dissertation, Swansea University]. <https://doi.org/10.23889/SUthesis.59027>
- Kleemans, E.R. (2014). Organized crime research: Challenging assumptions and informing policy. In J. Knutsson & E. Cockbain (Eds.), *Applied police research: Challenges and opportunities: Crime science series* (pp. 57-67). Willan Publishing.
- Kleinberg, B, Van der Vegt, I., & Gill, P (2020). The temporal evolution of a farright forum. *Journal of Computational Social Science*, 4. <https://doi.org/10.1007/s42001-020-00064-x>
- Kloess, J., & Van der Bruggen, M. (2021). Trust and relationship development among users in Dark Web Child sexual exploitation and abuse networks: A literature review from a psychological and criminological perspective. *Trauma, Violence & Abuse*. Advance online publication. <https://doi.org/10.1177/15248380211057274>
- Kleinrock, L. (2008). History of the internet and its flexible future. *IEEE Wireless Communications*, 15(1), 8-18. <https://doi.org/10.1109/MWC.2008.4454699>
- Krone, T. (2004). A typology of online child pornography offending. *Trends and Issues in Crime and Criminal Justice*, 279, 1-7.
- Krone, T., Spiranovic, C., Prichard, J., Watters, P., Wortley, R., Gelb, K., & Hunn, C. (2020). Child sexual abuse material in child-centred institutions: Situational crime prevention approaches. *Journal of Sexual Aggression*, 26(1), 91-110. <https://doi.org/10.1080/13552600.2019.1705925>
- Kokolaki, E., Daskalaki, E., Psaroudaki, K., Christodoulaki, M., & Fragopoulou, P. (2020). Investigating the dynamics of illegal online activity: The power of reporting, dark web, and related legislation. *Computer Law & Security Review*, 38. <https://doi.org/10.1016/j.clsr.2020.105440>

- Kruisbergen, E.W., Leukfeldt, E.R., Kleemans, E.R., & Roks, R.A. (2018). *Organised crime and IT: Empirical results of the fifth round of the Dutch Organised Crime Monitor*. WODC.
- Lacey, D., & Salmon P. (2015). It's dark in there: Using systems analysis to investigate trust and engagement in Dark Web forums. In D. Harris (Ed.), *Engineering Psychology and Cognitive Ergonomics. Lecture Notes in Computer Science*. Springer. [https://doi.org/10.1007/978-3-319-20373-7\\_12](https://doi.org/10.1007/978-3-319-20373-7_12)
- Lanning, K. (1986). Situational and preferential sex offenders. In M. Frost & M.J. Seng (Eds.), *Sexual Exploitation of the Child* (pp. 28-39). NCJ-104925.
- Lanning, K. (2001). Cyber pedophiles: A behavioral perspective. In R. Hazelwood & A.W. Burgess (Eds.), *Practical aspects of rape investigation: A multidisciplinary approach* (3<sup>rd</sup> ed., pp. 199-220). CRC Press.
- Lanning, K. (2010). *Child Molesters: A Behavioral Analysis*. NCMEC.
- Latapy, M., Magnien, C., & Del Vecchio, N. (2008). Basic notions for the analysis of large two-mode networks. *Social Networks*, 30(1), 31-48. <https://doi.org/10.1016/j.socnet.2007.04.006>
- Lavorgna, A., & Sergi, A. (2016). Serious, therefore organised? A critique of the emerging "cyber-organised crime" rhetoric in the United Kingdom. *International Journal of Cyber Criminology* 10(2), 170-187. <https://doi.org/10.5281/zenodo.163400>
- Leclerc, B., Drew, J., Holt, T., Cale, J., & Singh, S. (2021). Child sexual abuse material on the darknet: A script analysis of how offenders operate. *Trends & issues in crime and criminal justice*, 627, 1-14. <https://doi.org/10.52922/ti78160>
- Leclerc, B., Wortley, R., & Smallbone, S. (2011). Getting into the script of adult child sex offenders and mapping out situational prevention measures. *Journal of Research in Crime and Delinquency*, 48(2), 209-237. <https://doi.org/10.1177/0022427810391540>
- Leukfeldt, E.R. (2015). Organised cybercrime and social opportunity structures: A proposal for future research directions. *The European Review of Organised Crime*, 2(2), 91-103.
- Leukfeldt, E.R. (2016). *Cybercriminal networks: Origin, growth and criminal capabilities*. Eleven international Publishing.
- Leukfeldt, E.R., Kleemans, E., & Stol, W. (2016). Cybercriminal networks, social ties and online forums: Social ties versus digital ties within phishing and malware networks. *British Journal of Criminology*, 57(3), 704-722. <https://doi.org/10.1093/bjc/azw009>
- Leukfeldt, E.R., Lavorgna, A., & Kleemans, E.R. (2017). Organised cybercrime or cybercrime that is organised? An assessment of the conceptualisation of financial cybercrime as organised crime. *European Journal of Criminological Policy and Research*, 23(3), 287-300. <https://doi.org/10.1007/s10610-016-9332-z>

- Lievesley, R., Harper, C.A., & Elliott, H. (2020). The internalization of social stigma among minor-attracted persons: Implications for treatment. *Archives of Sexual Behavior*, 49, 1291–1304. <https://doi.org/10.1007/s10508-019-01569-x>
- Liggett, R., Lee, J.R., Roddy, A.L., & Wallin, M.A. (2020). The Dark Web as a platform for crime: An exploration of illicit drug, firearm, CSAM, and cybercrime markets. In T. Holt & A. Bossler (Eds.), *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (pp. 91–116). Springer International Publishing. [https://doi.org/10.1007/978-3-319-78440-3\\_17](https://doi.org/10.1007/978-3-319-78440-3_17)
- Lorenzo-Dus, N., Kinzel, A., & Cristofaro, M. (2020). The communicative modus operandi of online child sexual groomers: Recurring patterns in their language use. *Journal of Pragmatics*, 155, 15–27. <https://doi.org/10.1016/j.pragma.2019.09.010>
- Lusthaus, J. (2012). Trust in the world of cybercrime. *Global Crime*, 13(2), 71–94. <https://doi.org/10.1080/17440572.2012.674183>
- Lusthaus, J. (2013). How organised is organised cybercrime? *Global Crime*, 14(1), 52–60. <https://doi.org/10.1080/17440572.2012.759508>
- Lutz, C., & Hoffmann, C.P. (2017). The dark side of online participation: Exploring non-, passive and negative participation. *Information, Communication & Society*, 20(6), 876–897. <https://doi.org/10.1080/1369118X.2017.1293129>
- Malesky, L.A., & Ennis, L. (2004). Supportive distortions: An analysis of posts on a pedophile internet message board. *Journal of Addictions & Offender Counseling*, 24, 92–100. <https://onlinelibrary.wiley.com/doi/abs/10.1002/j.2161-1874.2004.tb00185.x>
- Markham, A.N. (2010). Internet research. In D. Silverman (Ed.), *Qualitative research: Theory, method, and practices* (3<sup>rd</sup> ed., pp. 111–127). SAGE.
- Martellozzo, E. (2015). Policing online child sexual abuse: The British experience. *European Journal of Policing Studies*, 3(1), 32–52.
- Martin, J. (2014). Lost on the Silk Road: Online drug distribution and the “cryptomarket.” *Criminology & Criminal Justice*, 14(3), 351–367. <https://doi.org/10.1177/1748895813505234>
- Maruna, S., & Mann, R.E. (2006). A fundamental attribution error? Rethinking cognitive distortions. *Legal and Criminological Psychology*, 11, 155–177. <https://onlinelibrary.wiley.com/doi/abs/10.1348/135532506X114608>
- Masson, K., & Bancroft, A. (2018). ‘Nice people doing shady things’: Drugs and the morality of exchange in the darknet cryptomarkets. *International Journal of Drug Policy*, 58, 78–84. <https://doi.org/10.1016/j.drugpo.2018.05.008>
- May, T. & Hough, M. (2004). Drug markets and distribution systems. *Addiction Research & Theory*, 12(6), 549–563. <https://doi.org/10.1080/16066350412331323119>
- Mazerolle, P., & McPhedran, S. (2019). Specialization and versatility in offending. In D.P. Farrington, L. Kazemian, & A.R. Piquero (Eds.), *The Oxford Handbook of Developmental and Life-Course Criminology*. Oxford University Press.

- Merdian, H.L., Curtis, C., Thakker, J., Wilson, N., & Boer, D.P. (2013). The three dimensions of online child pornography offending. *Journal of Sexual Aggression*, 19 (1), 121-132. <https://doi.org/10.1080/13552600.2011.611898>
- Miller, B. (2016). A computer-mediated escape from the closet: Exploring identity, community, and disinhibited discussion on an internet coming out advice forum. *Sexuality and Culture*, 20, 602-625. <https://link.springer.com/article/10.1007/s12119-016-9343-4>
- Morselli, C. (2009). Hells Angels in springtime. *Trends in Organized Crime*, 12, 145-158. <https://doi.org/10.1007/s12117-009-9065-1>
- Morselli, C., & Roy, J. (2008). Brokerage qualifications in ringing operations. *Criminology*, 46(1), 71-98. <https://doi.org/10.1111/j.1745-9125.2008.00103.x>
- Morzy, M. (2013). Evolution of online forum communities. In T. Özyer, J. Rokne, G. Wagner, & A. Reuser (Eds.), *The influence of technology on social network analysis and mining* (pp. 615-630). Springer.
- Mousavi, S., Roper, S., & Keeling, K. (2017). Interpreting social identity in online brand communities: Considering posters and lurkers. *Psychology and Marketing*, 34(4), 376-393. <https://doi.org/10.1002/mar.20995>
- Nagin, D.S. (2005). *Group-based modeling of development*. Harvard University Press.
- Nationaal Rapporteur (2021). *Dadermonitor seksueel geweld tegen kinderen 2015-2019*. Nationaal Rapporteur.
- National Crime Agency (2019). *National Strategic Assessment of Serious and Organised Crime*. <https://nationalcrimeagency.gov.uk/who-we-are/publications/296-national-strategic-assessment-of-serious-organised-crime-2019/file>
- Newman, M.E. (2001). Scientific collaboration networks. II. Shortest paths, weighted networks, and centrality. *Physical Review E*, 64(1). <https://doi.org/10.1103/PhysRevE.64.016132>
- Nolker, R.D., & Zhou, L. (2005). Social computing and weighting to identify member roles in online communities. *Proceedings of the 2005 IEEE/WIC/ACM International Conference on Web Intelligence*, 87-93. <https://doi.org/10.1109/WI.2005.134>
- Nonnecke, B., & Preece, J. (2000). Lurker demographics: Counting the silent. *Proceedings of the SIGCHI conference on Human Factors in Computing Systems*, 73-80. <https://doi.org/10.1145/332040.332409>
- Nurse, J., & Bada, M. (2018). The group element of cybercrime: Types, dynamics, and criminal operations. In A. Attrill-Smith, C. Fullwood, M. Keep, & D. Kuss (Eds.), *The Oxford Handbook of Cyberpsychology* (pp. 691-716). Oxford University Press.
- Ó Ciardha, C., & Ward, T. (2013). Theories of cognitive distortions in sexual offending: What the current research tells us. *Trauma, Violence, & Abuse*, 14, 5-21. <https://journals.sagepub.com/doi/10.1177/1524838012467856>

- O'Connell, R. (2001). Paedophiles networking on the Internet. In C.A. Arnaldo (Ed.), *Child abuse on the Internet: ending the silence* (pp. 65–80). Berghahn.
- Oerlemans, J.J. (2010). Een verborgen wereld: Kinderpornografie op internet. *Tijdschrift voor Familie- en Jeugdrecht*, 32(10), 236–243.
- O'Halloran, E., & Quayle, E. (2010). A content analysis of a “boy love” support forum: Revisiting Durkin and Bryant. *Journal of Sexual Aggression*, 16(10), 71–85. <https://doi.org/10.1080/13552600903395319>
- Owen, G., & Savage, N. (2015). *The Tor Dark Net*. Global Commission on Internet Governance. [https://www.cigionline.org/sites/default/files/no20\\_o.pdf](https://www.cigionline.org/sites/default/files/no20_o.pdf)
- Owen, G., & Savage, N. (2016). Empirical analysis of Tor Hidden Services. *IET Information Security* 10(3), 113–118. <https://doi.org/10.1049/iet-ifs.2015.0121>
- Owens, J., Eakin, J., Hoffer, T., Muirhead, Y., & Shelton, J.L.E. (2016). Investigative aspects of crossover offending from a sample of FBI online child sexual exploitation cases. *Aggression and Violent Behavior*, 30, 3–14. <https://doi.org/10.1016/j.avb.2016.07.001>
- Owens, J., Eakin, J., Hoffer, T., Muirhead, Y., & Shelton, J.L.E. (2016). Investigative aspects of crossover offending from a sample of FBI online child sexual exploitation cases. *Aggression and Violent Behavior*, 30, 3–14. <https://doi.org/10.1016/j.avb.2016.07.001>
- Özyer, T., Rokne, J., Wagner, J., & Reuser, A. (2013). *The influence of technology on social network analysis and mining*. Springer.
- Pannu, M., Kay, I., & Harris, D. (2019). Using Dark Web crawler to uncover suspicious and malicious websites. *Advances in Human Factors in Cybersecurity*, 782, 108–115. [https://doi.org/10.1007/978-3-319-94782-2\\_11](https://doi.org/10.1007/978-3-319-94782-2_11)
- Paoli, L. (2002). The paradoxes of organized crime. *Crime, Law and Social Change*, 37(1), 51–97.
- Paoli, L. (2003). *Mafia Brotherhoods: Organized crime, Italian style*. Oxford University Press.
- Paoli, L., & Beken, T. vander. (2014). Organized crime: A contested concept. In L. Paoli (Ed.), *The Oxford Handbook of Organized Crime* (pp. 13–31). Oxford University Press.
- Piquero, A.R., Farrington, D.P., & Blumstein, A. (2003). The criminal career paradigm. In M. Tonry (Ed.), *Crime and justice: A review of research* (pp. 359–506). University of Chicago Press.
- Piza, E., & Sytsma, V.A. (2016). Exploring the defensive actions of drug sellers in open-air markets: A systematic social observation. *Journal of Research in Crime and Delinquency*, 53(1), 36–65. <https://doi.org/10.1177/0022427815592451>
- Preece, J., Nonnecke, B., & Andrews, D. (2004). The top five reasons for lurking: Improving community experiences for everyone. *Computers in Human Behavior*, 20(2), 201–223. <https://doi.org/10.1016/j.chb.2003.10.015>

- Prichard, J., Watters, P., & Spiranovic, C. (2011). Internet subcultures and pathways to the use of child pornography. *Computer Law & Security Review*, 27(6), 585-600. <https://doi.org/10.1016/j.clsr.2011.09.009>
- Quayle, E., & Jones, T. (2011). Sexualised images of children on the internet. *Sexual Abuse: A Journal of Research and Treatment*, 23, 7-21. <https://doi.org/10.1177/1079063210392596>
- Quayle, E., & Taylor, M. (2003). Model of problematic internet use in people with a sexual interest in children. *CyberPsychology and Behavior*, 6(1), 93-106. <https://doi.org/10.1089/109493103321168009>
- Quayle, E., & Taylor, M. (2002). Child pornography and the internet: Perpetuating a cycle of abuse. *Deviant Behavior*, 23, 331-361. <https://www.tandfonline.com/doi/abs/10.1080/01639620290086413>
- Quinn, J.F., & Forsyth, C.J. (2013). Red light districts on blue screens: A typology for understanding the evolution of deviant communities on the internet. *Deviant Behavior* 34(7), 579-585. <https://doi.org/10.1080/01639625.2012.748629>
- Raven, A., Akhgar, B., & Abdel Samad, Y. (2021). Case studies: Child sexual exploitation. In B. Akhgar, M. Gercke, S. Vrochidis, & H. Gibson (Eds.), *Dark Web Investigation* (pp. 249-266). Springer.
- Rimer, J.R. (2017). Internet sexual offending from an anthropological perspective: Analysing offender perceptions of online spaces. *Journal of Sexual Aggression*, 23(1), 33-45. <https://doi.org/10.1080/13552600.2016.1201158>
- Rogers, M. (2003). The role of criminal profiling in the computer forensics process. *Computers & Security*, 22(4), 292-298. [https://doi.org/10.1016/S0167-4048\(03\)00405-X](https://doi.org/10.1016/S0167-4048(03)00405-X)
- Rutter, J., & Smith, G.W.H. (2005). Ethnographic presence in a nebulous setting. In C. Hine (Ed.), *Virtual methods: Issues in social research on the Internet* (pp. 81-92). Berg.
- Sammons, J. (2016). *Digital Forensics: Threatscape and Best Practices*. Elsevier inc.
- Schäfer, M., Fuchs, M., Strohmeier, M., Engel, M., Liechti, M., & Lenders, V. (2019). BlackWidow: Monitoring the dark web for cyber security information. *11th International Conference on Cyber Conflict (CyCon)*, 1-21. <https://doi.org/10.23919/CYCON.2019.8756845>
- Schelling, T. (1971). What is the business of organized crime? *Journal of Public Law* 20(1), 71-84.
- Seto, M.C., & Ahmed, A.G. (2014). Treatment and management of child pornography use. *Psychiatric Clinics of North America*, 37(2), 207-214. <https://doi.org/10.1016/j.psc.2014.03.004>
- Seto, M.C., Buckman, C., Dwyer, R.G., & Quayle, E. (2018). *Production and active trading of child sexual exploitation images depicting identified victims*. Missingkids.

- Seto, M.C., & Eke, A.W. (2005). The criminal histories and later offending of child pornography offenders. *Sexual Abuse: A Journal of Research and Treatment*, 17(2), 201-210. <https://doi.org/10.1007/s11194-005-4605-y>
- Seto, M.C., & Eke, A.W. (2015). Predicting recidivism among adult male child pornography offenders: Development of the child pornography offender risk tool (CPORT). *Law and Human Behavior*, 39(4), 416-429. <https://doi.org/10.1037/lhb0000128>
- Shelton, J., Eakin, J., Hoffer, T., Muirhead, Y., & Owens, J. (2016). Online child sexual exploitation: An investigative analysis of offender characteristics and offending behaviour. *Aggression and Violent Behavior*, 30, 15-23. <https://doi.org/10.1016/j.avb.2016.07.002>
- Simpson, E.H. (1949). Measurement of diversity. *Nature*, 163(4148), 688. <https://doi.org/10.1038/163688a0>
- Smid, W. (2014). *Sex offender risk assessment in the Netherlands: towards a risk need responsivity approach*. NL-ATSA.
- Soudijn, M. & Zegers, B. (2012). Cybercrime and virtual offender convergence settings. *Trends in Organized Crime*, 15(2-3), 111-129. <https://doi.org/10.1007/s12117-012-9159-z>
- Steel, C. (2009). Child pornography in peer-to-peer networks. *Child Abuse & Neglect*, 33(8), 56-568. <https://doi.org/10.1016/j.chiabu.2008.12.011>
- Steel, C., Newman, E., O'Rourke, S., & Quayle, E. (2020). An integrative review of historical technology and countermeasure usage trends in online child sexual exploitation material offenders. *Forensic Science International: Digital Investigation*, 33. <https://doi.org/10.1016/j.fsidi.2020.300971>
- St. Jean, P. (2007). *Pockets of crime: Broken windows, collective efficacy, and the criminal point of view*. University of Chicago Press.
- Tagarelli, A., & Interdonato, R. (2013). Who's out there? Identifying and ranking lurkers in social networks. *IEEE Xplore*, 1-8. <https://doi.org/10.1145/2492517.2492542>
- Taylor, M., Holland, G., & Quayle, E. (2001). Typology of paedophile picture collections. *The Police Journal*, 74, 97-107. <https://doi.org/10.1177/0032258X0107400202>
- Taylor, M. & Quale, E. (2003). *Child Pornography. An Internet Crime*. Brunner-Routledge.
- Telep, C.W. (2017). Police officer receptivity to research and evidence-based policing: Examining variability within and across agencies. *Crime & Delinquency*, 63(8), 976-999. <https://doi.org/10.1177/0011128716642253>
- Tener, D., Wolak, J., & Finkelhor, D. (2015). A typology of offenders who use online communications to commit sex crimes against minors. *Journal of Aggression, Maltreatment & Trauma*, 24(3), 319-337. <http://dx.doi.org/10.1080/10926771.2015.1009602>
- Tompson, L., & Chainey, S. (2011). Profiling illegal waste activity: Using crime scripts as a data collection and analytical strategy. *European Journal of Criminal Policy and Research*, 17(3), 179-201. <https://doi.org/10.1007/s10610-011-9146-y>

- Tyler, R., & Stone, L. (1985). Child pornography: Perpetuating the sexual victimization of children. *Child Abuse & Neglect*, 9(3), 313-318. [https://doi.org/10.1016/0145-2134\(85\)90026-2](https://doi.org/10.1016/0145-2134(85)90026-2)
- Tzanetakis, M., Kamphausen, G., Werse, B., & Laufenberg, R. von (2016). The transparency paradox. Building trust, resolving disputes and optimising logistics on conventional and online drugs markets. *International Journal on Drug Policy*, 35, 58-68. <https://doi.org/10.1016/j.drugpo.2015.12.010>
- Van der Bruggen, M. (2015). Een beschouwing van de ontwikkeling van het internet en cybercriminaliteit en de gevolgen hiervan voor de internationale bestrijding van digitale kinderporno. *Tijdschrift voor Criminologie*, 2, 242-259. <https://doi.org/10.5553/TvC/0165182X2015057002005>
- Van der Bruggen, M. (2018). Georganiseerde kinderpornonetwerken op het darkweb. *Justitiële Verkenningen*, 44(5), 40-53. <https://doi.org/10.5553/JV/016758502018044005004>
- 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>
- Van der Bruggen, M., & Blokland, A. (2021). Child sexual exploitation communities on the Darkweb: How organized are they? In M. Weulen Kranenbarg & R. Leukfeldt (Eds.), *Cybercrime in context: The human factor in victimization, offending, and policing* (pp. 259-280). Springer.
- Van der Bruggen, M., & Blokland, A. (2021). Profiling Darkweb child sexual exploitation material forum members using longitudinal posting history data. *Social Science Computer Review*, 40(4), 865-891. <https://doi.org/10.1177/0894439321994894>
- Van der Bruggen, M., Van Balen, I., Van Bunningen, A., Talens, P., Clapp, K., & Owens, J. (2022). Even “lurkers” download: The behavior and illegal activities of members on a child sexual exploitation Tor Hidden Service. *Aggression and Violent Behavior*, 67. <https://doi.org/10.1016/j.avb.2022.101793>
- Van Hout, M.C., & Bingham, T. (2013). Surfing the Silk Road: A study of users' experiences. *International Journal of Drug Policy*, 24(6), 524-529. <https://doi.org/10.1016/j.drugpo.2013.08.011>
- Van Remunt, T., & Van Wilsem, J. (2016). Wat wordt er nu eigenlijk gezegd? Een verkennend onderzoek naar communicatiepatronen op het Darkweb. *Proces*, 95(1), 24-39. <https://doi.org/10.5553/PRocES/016500762016095001004>
- Varese, F. (2010). What is organized crime? In F. Varese (Ed.), *Organized crime: Critical concepts in criminology* (pp. 1-33). Routledge.
- Von Lampe, K. (2016). *Organized crime: Analyzing illegal activities, criminal structures and extra-legal governance*. Sage.

- Von Lampe, K. (2016). The ties that bind: A taxonomy of associational criminal structures. In G.A. Antonopoulos (Ed.), *Illegal entrepreneurship, organized crime and social control* (pp. 19-35). Springer International Publishing.
- Von Lampe, K., & Johansen, P. (2003). Criminal networks and trust: On the importance of expectations of loyal behaviour in criminal relations. In S. Nevala, & K. Aromaa (Eds.), *Organised Crime, Trafficking, Drugs: Selected papers presented at the Annual Conference of the European Society of Criminology* (pp. 102-113). HEUNI.
- Von Lampe, K., & Johansen, P. (2004). Organized crime and trust: On the conceptualization and empirical relevance of trust in the context of criminal networks. *Global Crime*, 6(2), 159-184. <https://doi.org/10.1080/17440570500096734>
- Wall, D.S. (2007). *Cybercrime: The transformation of crime in the information age*. Polity Press.
- Ward, T., & Hudson, S.M. (2000). A self-regulation model of relapse prevention. In D.R. Laws, S.M. Hudson, & T. Ward (Eds.), *Remaking relapse prevention with sex offenders* (pp. 79-101). Sage.
- Webb, L., Craissati, J., & Kee, S. (2007). Characteristics of internet child pornography offenders: A comparison with child molesters. *Sexual Abuse*, 19, 449-465. <https://doi.org/10.1007/s11194-007-9063-2>
- Web-IQ (2018). *Web-IQ newsletter*. Web-IQ. <https://web-iq.com/news>
- Webster, S., Davidson, J., Bifulco, A., Gottschalk, P., Caretti, V., Pham, T., Grove-Hills, J., Turley, C., Tompkins, C., Ciulla, S., Milazzo, V., Schimmenti, A. & Craparo, G. (2012). *European online grooming project: Final report*. European Commission Safer Internet Plus Programme.
- Weimann, G. (2016). Going dark: Terrorism on the dark web. *Studies in Conflict & Terrorism*, 39(3), 195-206. <https://doi.org/10.1080/1057610X.2015.1119546>
- Wijsmuller, V. (2021). *Kinderporno op het Darkweb: Downloaders en keyplayers, wie zijn het?* [Dissertation, Politie Academie].
- WeProtect Global Alliance (2021). *Global Threat Assessment: Working together to end the sexual abuse of children online*. WeProtect Global Alliance.
- Westlake, B.G., & Bouchard, M. (2015). Criminal careers in cyberspace: Examining website failure within child exploitation networks. *Justice Quarterly*, 33(7), 1154-1181. <https://doi.org/10.1080/07418825.2015.1046393>
- Westlake, B.G., & Bouchard, M. (2016). Liking and hyperlinking: Community detection in online child sexual exploitation networks. *Social Science Research*, 59, 23-36. <https://doi.org/10.1016/j.ssresearch.2016.04.010>
- Westlake, B.G., Bouchard, M., & Frank, R. (2011). Finding the key players in online child exploitation networks. *Policy & Internet*, 3(2), 1-32. <https://doi.org/10.2202/1944-2866.1126>

- Wilson, G.D., & Cox, D.N. (1983). *The child-lovers: A study of paedophiles in society*. Peter Owen Publishers.
- Wilson, R., & Sandler, J. (2021). What works (or does not) in community risk management for persons convicted of sexual offenses? A contemporary perspective. *International Journal of Offender Therapy and Comparative Criminology*, 65(12), 1282–1298. <https://doi.org/10.1177/0306624X18754764>
- Winder, B., & Gough, B. (2010). “I never touched anybody – that’s my defence”: A qualitative analysis of internet sex offender accounts. *Journal of Sexual Aggression*, 16(2), 125–141. <https://www.tandfonline.com/doi/abs/10.1080/13552600903503383>
- Wolak, J., Liberatore, M., & Levine, B. (2014). Measuring a year of child pornography trafficking by U.S. computers on a peer-to-peer network. *Child Abuse & Neglect*, 38, 347–356. <https://doi.org/10.1016/j.chiabu.2013.10.018>
- Woodhams, J., Kloess, J., Brendan, J., & Hamilton-Giachritsis, C. (2021). Characteristics and behaviors of anonymous users of Dark Web platforms suspected of child sexual offenses. *Frontiers in Psychology*, 12, 1–11. <https://doi.org/10.3389/fpsyg.2021.623668>
- Yang, C., Ma, E., & Kao, D. (2021). Sexual offenses against children: Social learning theory and Dark Web reinforcement. *23rd International Conference on Advanced Communication Technology (ICACT)*, 449–454. <https://doi.org/10.23919/ICACT51234.2021.9370961>
- Yar, M. (2005). The novelty of ‘cybercrime’: an assessment in light of routine activity theory. *European Journal of Criminology*, 2(4), 407–427. <https://doi.org/10.1177/147737080556056>
- Yip, M., Shadbolt, N., & Webber, C. (2012). Structural analysis of online criminal social networks. In D. Zeng, L. Zhou, B. Cukic, G. Wang, & C. Yang (Eds.), *IEEE international conference on intelligence and security informatics (ISI)* (pp. 60–65). Piscataway.
- Yip, M., Webber, C., & Shadbolt, N. (2013). Trust among cybercriminals? Carding forums, uncertainty and implications for policing. *Policing and Society*, 23(4), 516–539. <https://doi.org/10.1080/10439463.2013.780227>
- Zanella, M. (2013). Script analysis of corruption in public procurement. In B. Leclerc & R. Wortley (Eds.), *Cognition and crime offender decision making and script analyses* (pp. 101–119). Routledge.
- Ziegel, E.R. (2001). Standard probability and statistics tables and formulae. *Technometrics*, 43(2), 249.
- Zulkarnine, A.T., Frank, R., Monk, B., Mitchell, J., & Davies, G. (2016). Surfacing collaborated networks in Dark Web to find illicit and criminal content. *Conference: 2016 IEEE Conference on Intelligence and Security Informatics (ISI)*, 1–6. <https://doi.org/10.1109/ISI.2016.7745452>

# SUMMARY

## **Child sexual abuse material networks on the Darkweb: A multi-method approach**

Because of the development of the internet and the associated digital opportunities, the crime of the possession and distribution of child sexual abuse material (CSAM) has gone through tremendous developments in the last decennia. Nowadays, many CSAM offenders access and distribute CSAM through the Darkweb, the hidden and encrypted part of the internet. This occurs on Darkweb CSAM fora, which have a sole focus on child sexual abuse. While the phenomenon of CSAM crime is not new, the fact that it now occurs on anonymous platforms like the Darkweb, has impacted the way these crimes are committed.

## **Research goal, research questions and method**

This dissertation is about CSAM networks on the Darkweb. Because of the illegal nature of Darkweb CSAM fora, empirical knowledge on their workings remains limited. Therefore, the overall objective of this dissertation is to describe and explain the criminal process and offender behavior on CSAM fora on the Darkweb. To do so, this dissertation applies insights from both the organized crime literature and from previous studies on individuals committing sexual offenses against children. A more practical aim of this effort is to offer professionals a more detailed insight into offenders' modus operandi, that can help to design more effective approaches for the identification, detection, assessment and treatment of CSAM offenders. In order to achieve the goal of this study, the following research questions were asked:

1. How can the criminal process of Darkweb CSAM fora be characterized?
2. How organized is the crime of CSAM on the Darkweb?
3. Which offender profiles and behavioral patterns can be distinguished on Darkweb CSAM fora?
4. How can keyplayers on Darkweb CSAM fora be identified?
5. How is trust on Darkweb CSAM fora established?

The main source of data used for this dissertation was (samples of) posts and threads from CSAM fora on the Darkweb. In all studies together, data from a total of six fora was used. The fora together had a total count of over 600,000 active forum members, and the data-sets included a total of approximately 760,000 posts. The timespan covered in the fora together was 2009-2017. Additionally, police investigations case files and suspect interviews were analyzed and interviews were conducted with police officers and public prosecutors.

A mix of qualitative as well as quantitative methods and multiple theoretical perspectives were used to answer the research questions. First, a crime script analysis (Cornish, 1994) was conducted in order to gain insight into the steps involved in the criminal process of Darkweb CSAM offending. Subsequently, a case file analysis of Dutch police investigations and accompanying interviews with professionals resulted in a study on the organization of CSAM on the Darkweb. Thirdly, various quantitative methods were used to determine offender profiles and to describe offender behavioral patterns on Darkweb CSAM fora. Quantitative methods used included Group-Based Trajectory Modeling (GBTM) (Jones & Nagin, 2013; Nagin, 2005) and various network science methods and techniques (Barabási, 2016). Finally, the concept of trust on Darkweb CSAM fora was analyzed by the means of a systematic literature review.

## Results

### ***The criminal process of Darkweb CSAM fora***

The criminal process of Darkweb CSAM offending can be subdivided into various phases (Chapter 2). In the first phase, preparations necessary to access the Darkweb CSAM forum are being made. Second, in the preactivity stage, members enter the forum for the first time. The third phase, the activity stage, consists of the actual execution of the main illegal act of exchanging CSAM. Finally, the postactivity stage consists of safely and securely exiting the crime scene and preventing detection. The most important characteristic of the criminal process of Darkweb CSAM offending is the continuous focus on technical security and support. Moreover, Darkweb CSAM offending entails more than the sole act of the online exchange of CSAM. Forum members not only discuss the CSAM exchanged on the forum, but forum discussions also include topics such as societal engagement, politics and media. In addition to online marketplaces, Darkweb CSAM fora can therefore be characterized as social communities.

An important distinction within this criminal process, is that between keyplayer members and general forum members. Keyplayer members often have a higher forum status, such as moderator or administrator, but they could also be 'regular' forum members who carry out important forum tasks. Keyplayers are much more active,

and often play a role in services important to the forum's establishment, maintenance and management. Technically, they invest much of their time to keep the forum safe and secure. Finally, keyplayers can decide about strategic changes to the forum, for example about its size and structure, entry requirements or branding and marketing. Contrarily, general forum members primarily use the forum's infrastructure for the exchange of CSAM and sometimes to communicate with like-minded others, but their role and activity are not pivotal for the forum's existence and development. These general forum members, especially the new ones, continuously need to be tutored in basic technical practicalities by more experienced forum members.

### ***The organization of CSAM crime on the Darkweb***

In order to study the organization of CSAM crime on the Darkweb (in Chapter 3), the flexible conception of organized crime from Von Lampe (2016) was used. Von Lampe (2016) distinguishes three types of social structures – entrepreneurial, associational and illegal governance structures – that may influence organized criminal activity.

Darkweb CSAM fora can firstly be characterized as digital marketplaces, or entrepreneurial structures, in which illegal goods in the form of CSAM are voluntarily exchanged and where there is overlap between suppliers and demanders. Like for actors in other criminal markets, there is a risk of exposure by law enforcement, and the need for security leads offenders to screen and get familiar with their co-offenders. In this insecure environment, some level of illegal governance, or enforcement of forum rules and regulations and the resolution of (internal) conflicts, is imposed by forum administrators. In 'business meetings' between forum administrators, decisions about such rules and responses to conflicts are being made. Another important task for forum administrators is to decide about arrangements between forum members served to protect them from threats such as government involvement or other outside attacks to the forum. Darkweb CSAM offending is further embedded in the social network between offenders, or the associational structure, provided by the forum environment. The shared sexual interest in children is the social tie that binds forum members, leading to an identification with the community, to unwritten internal social rules of and to the use of 'slang'. Although monetary profit, physical violence and the desire to monopolize the market (some traditional characteristics of organized crime) are largely absent, the criminal process of Darkweb CSAM offending as well as the offenders involved in it show clear signs of entrepreneurial and social organization.

### ***Offender profiles and behavioral patterns***

In this dissertation, six developmental pathways that can be interpreted as latent offender profiles, were distinguished (in Chapter 4):

1. The 'lurkers'. The largest group of forum members shows very little forum activity. Members allocated to this group enter the forum during its later stages and mostly refrain from posting shortly after entering.
2. The 'browsers'. This group also typically enters the forum in its later stages and portrays limited posting activity. Still, their average number of posts is almost five times higher than that of 'lurkers' and also includes posts under the 'Girls hardcore' forum environment category.
3. The 'CSAM interested'. This group has a longer posting duration and a higher average total of posts. The posting career of this group is more versatile in nature, and members allocated to this group often post under the 'Girls hardcore' and 'Boys hardcore' environments. Over half of the members in this category are registered as 'full member' by the forum administrators, suggesting that they contribute to the forum on a regular basis.
4. The 'escalators'. This group shows an increase in posting frequency the longer members are active on the forum. Given the timing of their last post, were the forum not taken offline, many members in this group likely would have continued to contribute to the forum. One in ten of the members allocated to this group has a VIP status.
5. The 'vested members'. Members of this group first become active already during the early stages of the forum's evolution and have a higher average total of posts in various sections of the forum. Their posting behavior signals their affinity with the (social) community as a whole. The large majority of members allocated to this group enjoy a 'full member' status, and over one fifth even has a VIP status.
6. The 'managers'. This final group is characterized by a high posting frequency. Members of this group do not only post under the 'General discussion' topic; three quarters also post under the 'Information and technical safety' topic, indicating that they are involved in the management of the forum in some way. Members in this group show the longest posting career, and over half of them have an Administrator or VIP status.

The results of this dissertation indicate that a small minority of forum members is responsible for the vast majority of the public forum communication. In other words, a large majority of forum members can be characterized as 'lurkers'. However, whereas these members show no verbal forum activity at all, they are still behaviorally active on the website and browse through the various forum environments. Furthermore, 93.6% of the forum members, of whom many 'lurking' members, are found to actively download CSAM. By their mere presence on the forum, 'lurkers' therefore also create and facilitate the demand and the market for CSAM (Chapter 5).

### ***Keyplayers on Darkweb CSAM fora***

Keyplayers can be automatically identified from large forum datasets using network metrics, such as various centrality measures (Chapter 6). More specifically, using these network science methods and techniques, the more individualistic role of technical keyplayer members dealing with the forum's establishment, encryption and maintenance can be revealed. Furthermore, structural properties and distributions of the topics discussed in and members active on the fora can be illuminated in this way. Insights in the forum's anti-lurker and anti-law enforcement policies and new member application guidelines, could be deduced only from looking at the network structure of the data. Distinguishing offender profiles and behavioral patterns and identifying keyplayers ultimately aids in the identification of the most active and dangerous Darkweb CSAM offenders, giving direction to law enforcement's prioritization in CSAM crime investigations.

### ***Trust establishment on Darkweb CSAM fora***

Although the concept of trust is not equally important to all forum members, and likely has the greatest value in explaining the behavior of the most active forum members; it is an important concept to comprehend how and why forum members communicate about their deepest sexual feelings online. Moreover, trust, to some extent, is necessary for two or more offenders to be willing to cooperate (Von Lampe, 2016).

Criminological studies, discussed in Chapter 7, highlight that on Darkweb CSAM fora trust initially needs to be established under circumstances of anonymity, without knowing the true identity of one's co-offenders. Information about others, and hence their level of trustworthiness, is therefore limited. The process of trust establishment may be enhanced by creating a legitimate and reliable online identity. Members share information about cybercriminal attributes, which then become a personal brand and as such lay the foundation for an online reputation that is necessary for trust to be developed further. Trust can be maintained by being visible and portraying oneself as an active member. This includes engaging in frequent online activity, involving posting messages, contributing to open discussions, exchanging valuable advice and by generally being helpful, as well as by mentoring and offering feedback to others. In addition, humor, playfulness, and sarcasm are frequently used to invoke trustworthiness. To conclude, within the high-stake and high-risk environment of the Darkweb, the associational structures of the fora lay an important foundation for trust to be established and maintained.

## Research strengths and limitations

The most important strength of this dissertation is its use of digital forensic artifacts. Online activities and behavior leave many more traces than do offline activities and behavior, offering a wealth of new data to be studied. This results in knowledge that could not – or at least not as reliably – be obtained without having access to these online data sources. Using Darkweb CSAM forum communication as a data source, enables to study a hard-to-reach population whose members are scarcely caught by law enforcement. Research into this hidden offender population through unobtrusive means allows to study the actual and ‘natural’ behavior of these individuals, thereby shedding unique light on concepts such as the criminal process, the criminal organization, as well as their motivation and trust establishment and maintenance. Moreover, using forum communication and forum member relationships as a data source enabled to study all forum members active on a Darkweb CSAM forum at once. In this world of big data, with Darkweb CSAM fora sometimes consisting of hundred thousands of members, sophisticated quantitative analyses become a necessary tool to gain insight into the fora’s structures and to identify the most important forum members.

Despite their strengths, the studies included in this dissertation also have some limitations. The first is related to the generalizability of the results. Though varied in size and structure, the fora used for the current analyses do not constitute a representative sample of all Darkweb CSAM fora in a statistical sense. Moreover, some potential crucial data was excluded from the current studies. The data available only covered forum communication posted on the public areas of the fora. Therefore, there was no way of estimating the size and nature of the private communication going on between members. Moreover, although general estimates of the type of CSAM exchanged on the various Darkweb fora under investigation were conducted, this dissertation did not include an assessment of the actual CSAM exchanged or collected through the fora and it did not use the material exchanged as unit of analysis. Finally, because of its sensitive nature, some of the data could be analyzed by one author only, which may have led to single coder bias.

## Academic and practical relevance

The use of digital forensic artifacts in this dissertation enabled to test theoretical constructs about criminal cooperation and the behavior of online sexual offenders, specifically for offenders active on Darkweb CSAM communities. Doing so, this dissertation offered a deeper as well as broader understanding of sexual offender theories, based on the growing population of online sexual offenders active on the Darkweb.

Although online activities and behavior leave many traces, and the accessibility of online data continues to grow, the possibilities to make this data available to researchers are still scant. This relates to challenges in making datasets containing material of an illegal nature available to researchers in a non-sensitive or derived way to allow them to study these data, as well as in challenges related to transform the often very large online datasets in analyzable formats. This dissertation relied on intensive cooperation with law enforcement personnel who have access to the relevant data and the clearance to view the actual material. The current research would simply have been impossible if such intensive cooperation could not be obtained. Having direct access to expertise within a specialized law enforcement unit, further enabled substantive interpretation of the results and hence, a deeper understanding of the data and the phenomenon under scrutiny. Therefore, in future research close cooperation between academic and law enforcement communities should be continued and reinforced.

From a practical point of view, this dissertation offers practical guidance and knowledge that may aid law enforcement in designing their investigations. Digital investigations, especially those on the hidden and anonymous Darkweb, are complex and time-consuming, and need a great deal of (technical) expertise and experience from law enforcement. Cooperation and close partnerships between academics and law enforcement communities are valuable in this regard. Law enforcement can provide academics with the most urgent questions to be answered in order for them to do their work effectively, and academics can feed law enforcement professionals with practical translations of the most recent research findings, including recommendations for a better practice. Finally, and most importantly, offending is inseparable from victimization. In other words, if there were no offenders, there would be no victims. Unfortunately, the impact of CSAM on its victims is often severe. Offender focused research, resulting in increased knowledge and recommendations for better intervention practice, ultimately contributes to a better protection of children.



# SAMENVATTING

## **Netwerken van seksueel kindermisbruik op het Darkweb: Een multi-methodische benadering**

Vanwege de ontwikkeling van het internet in de afgelopen decennia en de bijkomende digitale mogelijkheden, is de criminaliteit van het bezit en de verspreiding van kinderpornografisch materiaal – oftewel afbeeldingen van seksueel kindermisbruik – enorm veranderd. Afbeeldingen van seksueel kindermisbruik worden tegenwoordig vaak bekeken en verspreid op het Darkweb, het verborgen en versleutelde deel van het internet. Dit gebeurt op speciale Darkweb fora, die uitsluitend gericht zijn op kindermisbruik. Hoewel het fenomeen online seksueel kindermisbruik niet nieuw is, heeft het feit dat dit nu plaatsvindt op anonieme platformen zoals het Darkweb veel invloed op de manier waarop de criminaliteit gepleegd wordt.

## **Onderzoeksdoel, onderzoeksvragen en methode**

Dit proefschrift gaat over netwerken waar afbeeldingen van seksueel kindermisbruik gedeeld worden op het Darkweb. Vanwege het illegale karakter van dit soort Darkweb fora is de empirische kennis over hoe zij werken beperkt. Daarom is het doel van dit proefschrift om het criminele proces en het gedrag van individuen actief op deze fora te beschrijven en verduidelijken. Hiervoor wordt gebruikgemaakt van inzichten uit de literatuur van de georganiseerde misdaad en van eerder onderzoek naar daders van (online) zedendelicten jegens kinderen. Een bijgaand praktisch doel is om professionals beter inzicht te geven in de modus operandi van dit soort criminaliteit. Dit helpt in het ontwerpen van een effectieve aanpak voor de identificatie, detectie en de beoordeling en behandeling van daders. De volgende onderzoeksvragen zijn gesteld om dit doel te bereiken:

1. Hoe kan het criminele proces op fora over (afbeeldingen van) seksueel kindermisbruik op het Darkweb worden gekarakteriseerd?
2. Hoe georganiseerd zijn fora over (afbeeldingen van) seksueel kindermisbruik op het Darkweb?
3. Welke daderprofielen en gedragspatronen kunnen worden onderscheiden op fora over (afbeeldingen van) seksueel kindermisbruik op het Darkweb?

4. Hoe kunnen sleutelpersonen op fora over (afbeeldingen van) seksueel kindermisbruik op het Darkweb worden geïdentificeerd?
5. Hoe wordt vertrouwen op fora over (afbeeldingen van) seksueel kindermisbruik op het Darkweb gecreëerd?

De belangrijkste data die gebruikt zijn voor dit proefschrift zijn (steekproeven van) ‘posts’ en ‘threads’ afkomstig van fora over (afbeeldingen van) seksueel kindermisbruik op het Darkweb. In totaal zijn voor alle hoofdstukken in dit proefschrift zes fora gebruikt. Gezamenlijk hadden deze fora meer dan 600,000 actieve leden, en de datasets bevatten in totaal ongeveer 760,000 posts. De tijdsperiode waarin deze fora online waren betrof 2009-2017. Daarnaast zijn dossiers van politieonderzoeken en verslagen van verdachtenverhoren geanalyseerd en er zijn interviews gehouden met politiemedewerkers en officieren van justitie.

Een mix van kwalitatieve en kwantitatieve onderzoeksmethoden en verschillende theoretische perspectieven zijn gebruikt om de onderzoeksvragen te beantwoorden. Allereerst is een ‘crime script analyse’ (Cornish, 1994) verricht om inzicht te bieden in de verschillende stappen van het criminele proces dat ten grondslag ligt aan fora over (afbeeldingen van) seksueel kindermisbruik op het Darkweb. Daarna is een studie verricht naar de criminele organisatie van fora over (afbeeldingen van) seksueel kindermisbruik op het Darkweb. Hiervoor zijn de dossiers van politieonderzoeken en de interviews met betrokken politiemedewerkers en officieren van justitie geanalyseerd. Vervolgens zijn verschillende kwantitatieve methoden gebruikt om daderprofielen te onderscheiden en om gedrag patronen van deze daders op de fora te beschrijven. De kwantitatieve methoden die gebruikt zijn, zijn de ‘Group-Based Trajectory Modeling’ (GBTM) (Jones & Nagin, 2013; Nagin, 2005) en verschillende ‘network science’ methoden en technieken (Barabási, 2016). Tot slot is het concept van vertrouwen onderzocht aan de hand van een systematisch literatuuronderzoek.

## Resultaten

### ***Het criminele proces van fora over (afbeeldingen van) seksueel kindermisbruik op het Darkweb***

Het criminele proces dat ten grondslag ligt aan fora over (afbeeldingen van) seksueel kindermisbruik op het Darkweb kan onderverdeeld worden in verschillende fasen (zie hiervoor meer in Hoofdstuk 2). In de eerste fase worden voorbereidingen getroffen om een dergelijk forum op het Darkweb te kunnen vinden en benaderen. In de tweede fase betreden forumleden het forum voor de eerste keer. De derde fase

betreft het daadwerkelijk plegen van strafbare feiten: het bekijken en uitwisselen van kinderpornografisch materiaal. In de laatste fase verlaten daders op een veilige wijze de plaats delict (het forum) op een manier waarop detectie voorkomen wordt. Het belangrijkste kenmerk van het criminele proces is de continue focus op technische beveiliging en ondersteuning. Daarnaast bevat daderschap op fora over (afbeeldingen van) seksueel kindermisbruik meer dan het simpelweg online uitwisselen van afbeeldingen van seksueel kindermisbruik. Op fora worden onderwerpen als maatschappelijk en politiek engagement, en media uitlatingen ook veelvuldig besproken. Daarnaast vinden er veel sociale gesprekken plaats. Naast online marktplaatsen, kunnen fora dus ook gekarakteriseerd worden als online sociale gemeenschappen.

Een belangrijk onderscheid in dit criminele proces is dat tussen keyplayers en reguliere forumleden. Keyplayers hebben vaak een hogere formele status op het forum, zoals ‘moderator’ of ‘administrator’, maar zij kunnen ook een eenvoudige status hebben als ‘registered member’ maar wel verantwoordelijke taken voor het forum uitvoeren. Keyplayers zijn vaak veel actiever, en hebben een verantwoordelijkheid in de oprichting, het onderhoud en het beheer van het forum. Vanuit technisch perspectief, investeren zij veel tijd in het veilig houden van het forum. Tot slot nemen keyplayers beslissingen over strategische veranderingen binnen het forum, bijvoorbeeld over de forumstructuur, toelatingseisen van leden, en over marketing. Reguliere forumleden daarentegen, gebruiken het forum met name voor het uitwisselen van afbeeldingen van seksueel kindermisbruik en soms voor het communiceren met andere forumleden. Hun rol is echter niet doorslaggevend voor het bestaan en de ontwikkeling van het forum. Reguliere leden, en met name de nieuwe forumleden, worden onderwezen in de technische basisvaardigheden door de meer ervaren forumleden.

### ***De organisatie van fora over (afbeeldingen van) seksueel kindermisbruik op het Darkweb***

Om de (criminele) organisatie van fora over (afbeeldingen van) seksueel kindermisbruik op het Darkweb te kunnen bestuderen (in Hoofdstuk 3), is de flexibele definitie van de georganiseerde misdaad van Von Lampe (2016) gebruikt. Von Lampe (2016) onderscheidt drie soorten sociale structuren – ‘entrepreneurial’, ‘associational’ en ‘illegal governance’ structuren – die georganiseerde criminele activiteit beïnvloeden.

Fora over (afbeeldingen van) seksueel kindermisbruik op het Darkweb kunnen worden gekarakteriseerd als digitale marktplaatsen (‘entrepreneurial’ structuren), waar illegaal materiaal vrijwillig uitgewisseld wordt en waar overlap is tussen vraag en aanbod. Zoals bij andere criminele marktplaatsen is er een risico om ontmanteld te worden door de politie. Dit leidt tot de noodzaak van (technische) veiligheid en van het screenen en leren kennen van mededaders. In deze onzekere omgeving wordt de handhaving van forumregels en het oplossen van (interne) conflicten geregeld door forum administrators.

In zogenaamde ‘business meetings’ tussen deze administrators worden keuzes gemaakt over deze ‘governance’ van het forum. Daarnaast dragen administrators zorg voor de bescherming van het forum en haar leden tegen bedreigingen, zoals politie-invallen of andere externe aanvallen op het forum. De criminaliteit op fora over (afbeeldingen van) seksueel kindermisbruik op het Darkweb is verder ingebed in het sociale netwerk tussen de daders onderling (de ‘associational’ structuur). Hun gezamenlijke seksuele interesse in kinderen verbindt forumleden op sociaal vlak, en leidt tot de identificatie van forumleden met de sociale gemeenschap en tot ongeschreven sociale regels en het gebruik van ‘slang’. Hoewel geldelijk gewin, fysiek geweld en de wens tot het monopoliseren van de markt (de traditionele kenmerken van de georganiseerde misdaad) grotendeels afwezig zijn, hebben het criminele proces van fora over (afbeeldingen van) seksueel kindermisbruik op het Darkweb en de daders die hierbij betrokken zijn belangrijke kenmerken van een zakelijke en sociale organisatie.

### ***Daderprofielen en gedragspatronen***

Dit proefschrift onderscheidt zes ontwikkelingspaden, die geïnterpreteerd kunnen worden als latente daderprofielen (zie hiervoor meer in Hoofdstuk 4):

1. De ‘lurkers’. De grootste groep forumleden is het minst actief en post zeer weinig berichten. Deze leden betreden het forum voor het eerst als het forum al langere tijd online is.
2. De ‘browsers’. Ook leden behorend tot deze groep betreden het forum voor het eerst als het forum al langere tijd online is en posten weinig berichten. Echter, hun frequentie van posten is alsnog vijf keer zo hoog als dat van lurkers en er wordt door deze groep ook gepost in de ‘Girls hardcore’ forumomgeving.
3. De ‘CSAM interested’.<sup>1</sup> Deze groep post gemiddeld gezien meer berichten over een langere periode. De posting carrière van leden die bij deze groep horen is bovendien veelzijdiger, en zij posten regelmatig in de ‘Girls hardcore’ en ‘Boys hardcore’ forumomgevingen. Meer dan de helft van de leden behorend bij deze groep hebben een formele forumstatus als ‘full member’, wat betekent dat zij op regelmatige basis bijdragen aan het forum.
4. De ‘escalators’. De frequentie van posten van berichten neemt toe naarmate leden behorend tot deze groep langer actief zijn op het forum. Het moment waarop hun laatste post geplaatst werd, laat zien dat forumleden uit deze groep waarschijnlijk actief waren gebleven op het forum, als het forum niet offline gehaald was. Een tiende van de leden van deze groep heeft een ‘VIP status’.

---

<sup>1</sup> CSAM staat voor Child Sexual Abuse Material, oftewel afbeeldingen van seksueel kindermisbruik.

5. De 'vested members'. De forumleden behorend bij deze groep worden lid van het forum op het moment dat het forum nog maar net online is. Daarnaast hebben ze een hoog gemiddeld aantal posts die geplaatst worden binnen verschillende forumomgevingen. Bovendien laat hun postinggedrag zien dat deze leden begaan zijn met de sociale gemeenschap. Het grootste deel van deze forumleden heeft een formele forumstatus als 'full member' en ruim een vijfde heeft een 'VIP status'.
6. De 'managers'. Deze laatste groep is het meest actief en kent de grootste frequentie van posts. Leden behorend bij deze groep posten niet alleen onder de 'General discussion' forumomgeving, maar drie kwart van hen post ook in de 'Information and technical safety' omgeving, wat laat zien dat deze leden betrokken zijn bij het forum management. Meer dan de helft van de leden binnen deze groep heeft een 'Administrator' of 'VIP status'.

Uit de resultaten van dit proefschrift blijkt dat een kleine minderheid van forumleden verantwoordelijk is voor het grootste deel van alle publieke forumcommunicatie. Een zeer groot deel van de forumleden kan dus gekarakteriseerd worden als 'lurker'. Maar hoewel deze forumleden (vrijwel) geen verbale communicatie tentoonspreiden op het forum, blijkt uit dit proefschrift dat zij alsnog actief zijn op het forum door rond te browsen in de verschillende forumomgevingen. Daarnaast blijkt dat 93,6% van de forumleden – waaronder een groot aantal 'lurkers' – actief afbeeldingen van seksueel kindermisbruik downloadt. Simpelweg hun aanwezigheid op het forum zorgt dus voor het aanwakkeren en faciliteren van de vraag naar en het aanbod van afbeeldingen van seksueel kindermisbruik (zie hiervoor meer in Hoofdstuk 5).

### ***Keyplayers op fora over (afbeeldingen van) seksueel kindermisbruik op het Darkweb***

Door middel van netwerkstatistieken, zoals centraliteitsmaten, kunnen keyplayers automatisch worden geïdentificeerd uit grote forumdatasets (zie hiervoor meer in Hoofdstuk 6). Met het gebruik van deze 'network science' methoden en technieken kon de individualistische rol van de technische keyplayer, die zorgdraagt voor het bouwen van het forum, en de beveiliging en het onderhoud ervan, worden aangewezen. Daarnaast konden eigenschappen van de structuren van de posts en threads op het forum en de discussieonderwerpen worden geïdentificeerd. Met enkel het analyseren van de netwerkstructuur van de data, werden het anti-lurker en anti-politie beleid van het forum en richtlijnen voor forumleden inzichtelijk gemaakt. Het onderscheiden van daderprofielen, gedragspatronen en keyplayers op automatische wijze is van groot belang om de meest actieve en gevaarlijke forumleden efficiënt te kunnen identificeren. Deze werkwijze geeft richting aan het prioriteringsproces in politieonderzoeken naar online seksueel misbruik.

### ***Vertrouwen op fora over (afbeeldingen van) seksueel kindermisbruik op het Darkweb***

Hoewel vertrouwen niet voor alle forumleden even belangrijk is, en naar alle waarschijnlijkheid het meest belangrijk is voor de samenwerking tussen de actievere forumleden; is het concept belangrijk om te begrijpen waarom en hoe forumleden online over hun diepste seksuele gevoelens praten. Daarnaast is vertrouwen tot een zeker niveau noodzakelijk als twee of meer daders met elkaar willen samenwerken (Von Lampe, 2016).

Uit criminologische studies, besproken in Hoofdstuk 7, blijkt dat vertrouwen op fora over (afbeeldingen van) seksueel kindermisbruik op het Darkweb in eerste instantie wordt gecreëerd onder anonieme omstandigheden, waarbij de echte identiteit van mededaders onbekend is. De informatie over mededaders en de mate waarin zij vertrouwd kunnen worden, is dus nog onbekend. Het proces van het creëren van vertrouwen gaat gemakkelijker wanneer een dader een betrouwbare online identiteit heeft. Een betrouwbare identiteit ontstaat bijvoorbeeld door het delen van informatie over het criminele verleden en vaardigheden. Deze informatie, gelinkt aan de nickname van een forumlid, wordt een ‘personal brand’ dat de basis legt voor een online reputatie die noodzakelijk is voor de groei van vertrouwen. Het vertrouwen kan vervolgens behouden worden door zichtbaar en actief te zijn op het forum. Hierbij gaat het bijvoorbeeld om het frequent posten van berichten, het deelnemen aan publieke discussies, en om behulpzaam zijn, bijvoorbeeld door het delen van advies en feedback aan medeforumleden. Daarnaast blijken humor, speelsheid en sarcasme bij te dragen aan de groei van vertrouwen. Concluderend kan gesteld worden dat de sociale omgeving van een forum een belangrijke basis legt voor het creëren en behouden van vertrouwen in een in de basis risicovolle en onveilige omgeving.

## **Onderzoeksbependingen en mogelijkheden voor toekomstig onderzoek**

De belangrijkste kracht van dit proefschrift is het gebruik van ‘digital forensic artifacts’. Online activiteiten en gedrag laten veel meer sporen na dan offline activiteiten en gedrag, wat zorgt voor een veelheid aan nieuwe data die door onderzoekers geanalyseerd kunnen worden. Dit resulteert in kennis die niet – of in ieder geval niet zo betrouwbaar – gegenereerd had kunnen worden zonder toegang tot deze online databronnen. Het gebruik van Darkweb forumcommunicatie over (afbeeldingen van) seksueel kindermisbruik als databron maakt het mogelijk om een verborgen daderpopulatie, (nog) niet in beeld van politie en justitie, te onderzoeken. Onderzoek naar deze verborgen daderpopulatie maakt het mogelijk om het feitelijke en ‘natuurlijke’

gedrag van deze personen te bestuderen, wat een uniek licht werpt op concepten zoals het criminele proces, de criminele organisatie, evenals dadermotivatie en onderling vertrouwen. Het gebruik van forumcommunicatie en relaties tussen forumleden als databron maakte het daarnaast mogelijk om alle forumleden tegelijkertijd te bestuderen. Het feit dat fora over (afbeeldingen van) seksueel kindermisbruik op het Darkweb vaak honderdduizenden leden hebben maakt geavanceerde kwantitatieve technieken noodzakelijk om inzicht te krijgen in de forumstructuren en om de belangrijke forumleden te kunnen identificeren.

Desondanks kennen de studies uit dit proefschrift ook enkele beperkingen. De eerste betreft de generaliseerbaarheid van de resultaten. Hoewel bewust gekozen is voor fora die variëren in grootte en structuur, zijn de fora uit dit proefschrift statistisch gezien niet representatief voor alle fora over (afbeeldingen van) seksueel kindermisbruik op het Darkweb. Daarnaast zijn cruciale data niet meegenomen in dit proefschrift. Zo bevatten de datasets alleen de forumcommunicatie afkomstig uit de publieke onderdelen van de fora. Dit betekent dat er geen inzicht is in de privé communicatie tussen forumleden onderling. En hoewel er wel algemene schattingen zijn gemaakt van het type afbeeldingen uitgewisseld op de onderzochte fora, bevatte dit proefschrift geen gedetailleerde beoordeling van het daadwerkelijk uitgewisselde materiaal en is het uitgewisselde materiaal niet gebruikt als analyse-eenheid. Ten slotte konden sommige datasets, vanwege de gevoelige aard ervan, door slechts één auteur worden geanalyseerd, waardoor geen interbeoordelaarsbetrouwbaarheid gemeten kon worden.

## **Academische en praktische relevantie**

Het gebruik van ‘digital forensic artifacts’ in dit proefschrift maakte het mogelijk om theorieën over criminele samenwerking en het gedrag van online zedendelinquenten te testen voor daders actief op fora over (afbeeldingen van) seksueel kindermisbruik op het Darkweb. Hiermee biedt dit proefschrift zowel een dieper als breder inzicht in theorieën over zedencriminaliteit, gebaseerd op de groeiende populatie van daders actief op fora over (afbeeldingen van) seksueel kindermisbruik op het Darkweb.

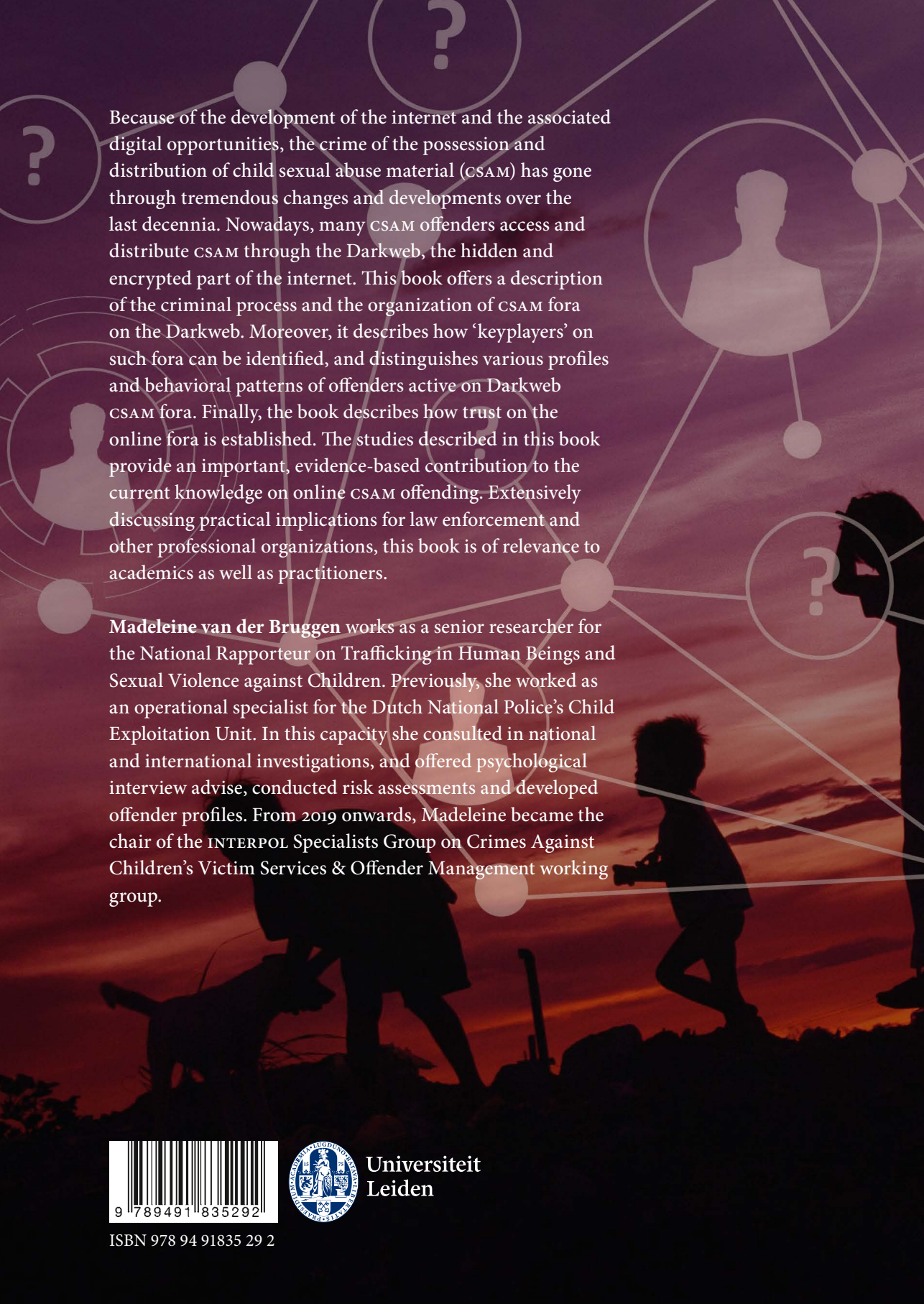
Zoals gezegd laten online activiteiten en gedrag veel sporen na, en er is sprake van een toename van online data. Ondanks dit zijn de mogelijkheden om dit soort data beschikbaar te stellen voor onderzoek nog steeds beperkt. Dit komt doordat het lastig is om illegale data op een ethische manier beschikbaar te stellen voor onderzoekers. Daarnaast zijn er uitdagingen verbonden aan het transformeren van de – vaak grote – datasets in formats die analyseerbaar zijn. Het onderzoek dat geresulteerd heeft in

dit proefschrift kende een zeer nauwe en intensieve samenwerking met politiemedewerkers die toegang hebben tot de data en die zijn gevrijwaard om deze data te mogen bekijken en analyseren. Dit onderzoek was onmogelijk geweest zonder een dergelijke intensieve samenwerking. Daarnaast maakte de directe toegang tot gespecialiseerd politiepersoneel diepgaande interpretatie van de onderzoeksresultaten mogelijk, wat geleid heeft tot een groter begrip van de data en van het fenomeen zelf. Hieruit kan geconcludeerd worden dat nauwe samenwerking tussen de wetenschap en de politie voortgezet en versterkt moet worden in toekomstig onderzoek.

Vanuit praktijkperspectief geeft dit proefschrift richting en praktische kennis die de politie kan helpen in het ontwerpen en plannen van hun onderzoeken. Digitaal onderzoek, met name op het verborgen en anonieme Darkweb, is complex en tijdrovend, en hiervoor is aanzienlijke (technische) expertise en ervaring nodig. Ook in dit perspectief is nauwe samenwerking tussen de politie en wetenschap belangrijk. De politie kan de wetenschap voorzien van de meest prangende onderzoeksvragen die zij beantwoord willen zien om hun werk effectief te kunnen uitvoeren. En daarnaast kan de wetenschap de politie voeden met praktische vertalingen van de meest recente onderzoeksbevindingen, waaronder aanbevelingen voor een efficiëntere aanpak. Tot slot kan daderschap niet los gezien worden van slachtofferschap. Met andere woorden, zonder daders zouden er geen slachtoffers zijn. De impact van seksueel kindermisbruik op de slachtoffers is groot. Dadergericht onderzoek, dat resulteert in kennis over en aanbevelingen voor het voorkomen en signaleren van daderschap, draagt uiteindelijk ook bij aan een betere bescherming van kinderen.

# CURRICULUM VITAE

Madeleine van der Bruggen was born in 1986 in Tilburg. She received her Master's degree in Criminology at Utrecht University in 2008 and her Master's degree in Forensic Psychology at Coventry University (United Kingdom) in 2012. After having been employed at Terrence Higgins Trust, where she offered support to sex workers and was the project leader for a research program into sex work in the Warwickshire area, she moved back to the Netherlands. From 2013 onwards, she worked as an operational specialist for the Dutch National Police's Child Exploitation Unit. In this capacity she consulted in national and international investigations, and offered psychological interview advice, conducted risk assessments and developed offender profiles. From 2016-2022, Madeleine worked on her PhD-study into child sexual abuse material networks on the Darkweb at Leiden Law School of Leiden University. From 2019 onwards, she has been working as a senior researcher for the National Rapporteur on Trafficking in Human Beings and Sexual Violence against Children. Finally, Madeleine is currently the chair of the INTERPOL Specialists Group on Crimes Against Children's Victim Services & Offender Management working group.



Because of the development of the internet and the associated digital opportunities, the crime of the possession and distribution of child sexual abuse material (CSAM) has gone through tremendous changes and developments over the last decennia. Nowadays, many CSAM offenders access and distribute CSAM through the Darkweb, the hidden and encrypted part of the internet. This book offers a description of the criminal process and the organization of CSAM fora on the Darkweb. Moreover, it describes how 'keyplayers' on such fora can be identified, and distinguishes various profiles and behavioral patterns of offenders active on Darkweb CSAM fora. Finally, the book describes how trust on the online fora is established. The studies described in this book provide an important, evidence-based contribution to the current knowledge on online CSAM offending. Extensively discussing practical implications for law enforcement and other professional organizations, this book is of relevance to academics as well as practitioners.

**Madeleine van der Bruggen** works as a senior researcher for the National Rapporteur on Trafficking in Human Beings and Sexual Violence against Children. Previously, she worked as an operational specialist for the Dutch National Police's Child Exploitation Unit. In this capacity she consulted in national and international investigations, and offered psychological interview advice, conducted risk assessments and developed offender profiles. From 2019 onwards, Madeleine became the chair of the INTERPOL Specialists Group on Crimes Against Children's Victim Services & Offender Management working group.



ISBN 978 94 91835 29 2



Universiteit  
Leiden