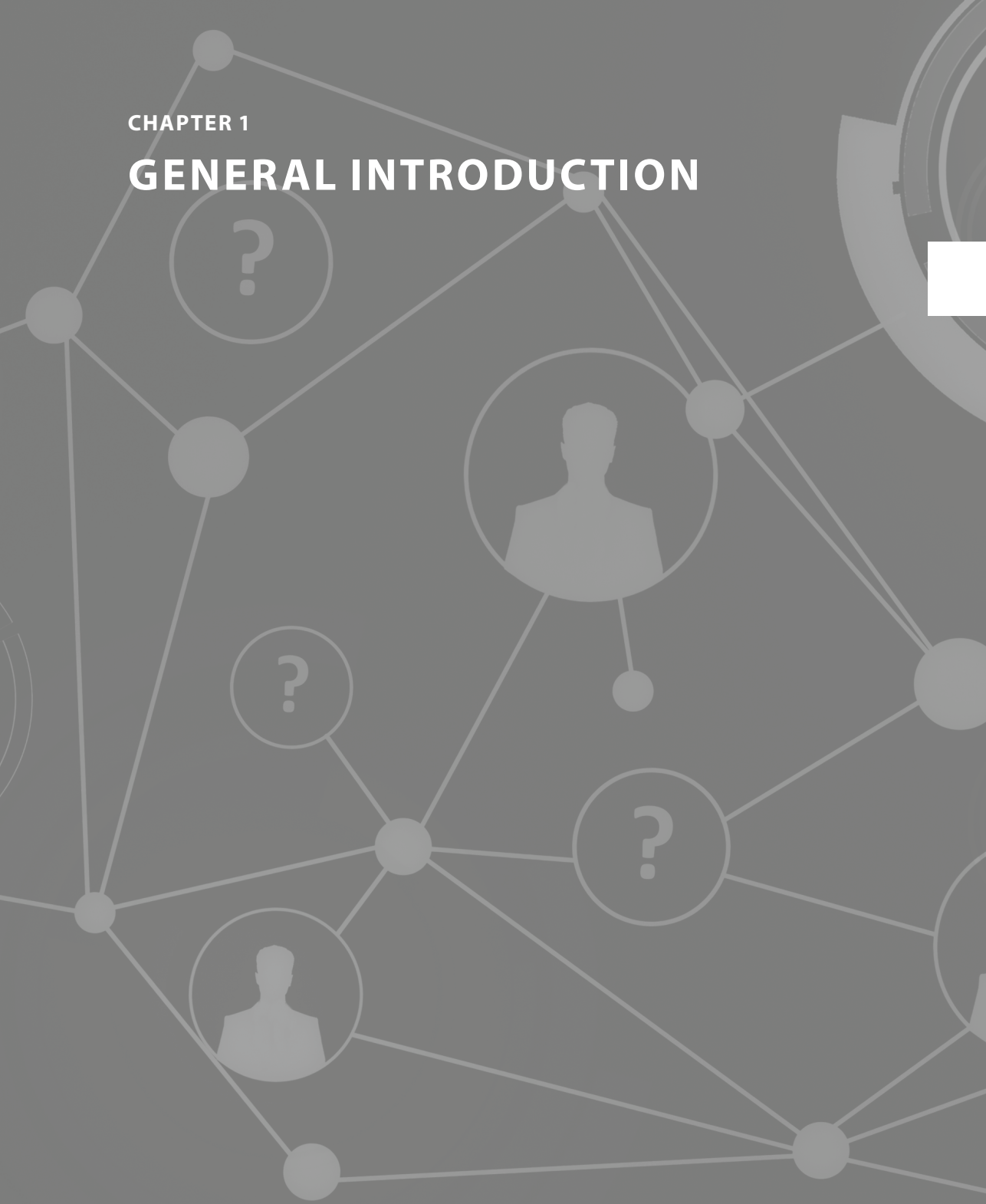
Child sexual abuse material networks on the darkweb: a multi-method approach

Bruggen, M. van der

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.[1] 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.[2] 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.[3] 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.[4]

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-gywcps.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; Wijsmuller, 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 voluntary 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.[5] CSAM is in this regard defined as any material depicting sexually explicit activities involving a child,

5 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[a]	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

[a] 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 be 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 ads 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.