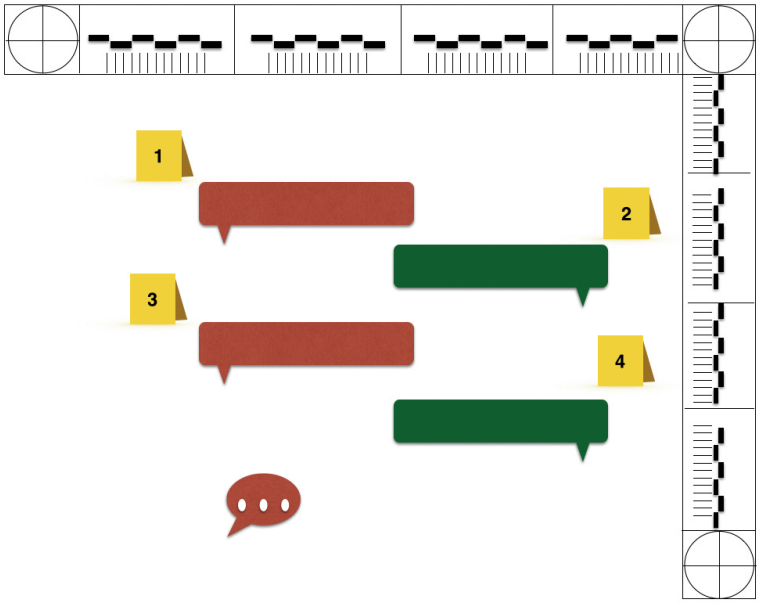
JYU DISSERTATIONS 164

Manja Nikolovska

The Internet as a Creator of a Criminal Mind and Child Vulnerabilities in the Cyber Grooming of Children



UNIVERSITY OF JYVÄSKYLÄ
FACULTY OF INFORMATION TECHNOLOGY

JYU DISSERTATIONS 164

Manja Nikolovska

The Internet as a Creator of a Criminal Mind and Child Vulnerabilities in the Cyber Grooming of Children

Esitetään Jyväskylän yliopiston informaatioteknologian tiedekunnan suostumuksella
julkisesti tarkastettavaksi yliopiston vanhassa juhlasalissa S212
helmikuun 7. päivänä 2020 kello 12.

Academic dissertation to be publicly discussed, by permission of
the Faculty of Information Technology of the University of Jyväskylä,
in building Seminarium, auditorium S212, on February 7, 2020 at 12 o'clock noon.

JYVÄSKYLÄN YLIOPISTO
UNIVERSITY OF JYVÄSKYLÄ

JYVÄSKYLÄ 2020

Editors
Marja-Leena Rantalainen
Faculty of Information Technology, University of Jyväskylä
Ville Korkiakangas
Open Science Centre, University of Jyväskylä

Cover picture by Manja Nikolovska.

Permanent link to this publication: http://urn.fi/URN:ISBN:978-951-39-7963-8

ISBN 978-951-39-7963-8 (PDF)
URN:ISBN:978-951-39-7963-8
ISSN 2489-9003

ABSTRACT

Nikolovska, Manja
The Internet as a creator of a criminal mind and child vulnerabilities in the cyber grooming of children
Jyväskylä: University of Jyväskylä, 2020, 145 p.
(JYU Dissertations
ISSN 2489-9003; 164)
ISBN 978-951-39-7963-8 (PDF)

Cyber grooming of children is a form of online child sexual abuse and a cybercriminal phenomenon on the rise. The previous literature explains this phenomenon by applying theories developed for the physical world, continuum models of offender and victim behavior, or process models of the act. This literature is silent on empirically addressing the role of cyber-specific behavioral variables in the cyber-grooming process, as expressed by both the offender and victim.

This dissertation maintains that until we gain an empirical understanding of how cyber-specific behavioral characteristics are being used by the offender and victim in the cyber-grooming process, we cannot offer a detailed explanation of online child sexual abuse. For this purpose, this research conceptualizes cyber affordances as cyber-specific variables to be measured within chat-interactive cybercriminal incidents. The conceptual model is applied to empirical data of real-life cases of cyber grooming of children. The study unveils the most critical incidents occurring in the chats, the offender's and victim's dynamic fluctuation in the cyber-grooming process, and the use of cyber affordances in relation to the cyber-grooming process. The study provides directions for future research and practical implications for preventing cyber grooming and cybercrime.

Keywords: cyber grooming; cyber affordances; content analysis: cybercrime; prevention

TIIVISTELMÄ

Nikolovska, Manja
Internet ja verkkoympäristöt uudenlaisen rikollisuuden ja lasten seksuaalisen hyväksikäytön mahdollistajana
Jyväskylä: University of Jyväskylä, 2020, 145 p.
(JYU Dissertations
ISSN 2489-9003; 164)
ISBN 978-951-39-7963-8 (PDF)

Verkossa tapahtuva grooming (engl. cyber grooming) eli *seksuaalinen nettihoukuttelu* on kasvava ilmiö. Sillä tarkoitetaan internetin välityksellä tapahtuvaa lapsen tai nuoren houkuttelua, jonka seurauksena hyväksikäyttäjä voi onnistua johdattamaan lapsen tai nuoren seksuaaliseen kanssakäymiseen kanssaan.
Aiempi tutkimus on soveltanut ilmiöön sellaisia rikosta, tekijöitä tai uhreja koskevia teorioita, jotka on alun perin kehitetty nettiä varhaisemman rikollisuuden selittämiseksi. Tämän väitöstutkimuksen havaintojen mukaan seksuaalisen nettihoukuttelun vaiheita ja syitä ei kuitenkaan kyetä kuvaamaan tarpeeksi syvällisesti ennen kuin meillä on lisää empiirisiä löydöksiä, jotka auttavat meitä valottamaan ilmiötä ja sen syntyä tarkemmin.

Tässä tutkimuksessa verkko- eli kybermaailman käyttömahdollisuudet käsitteellistetään tarkemmiksi kyberspesifeiksi muuttujiksi, joita voidaan tarkemmin kvantitatiivisesti määrittää interaktiivisissa verkkorikostapahtumissa. Tätä mallia sovelletaan todelliseen lapsiin kohdistuvista seksuaalisista nettihoukuttelurikoksista koostuvaan aineistoon. Tutkimuksessa selvitetään keskeisimmät chatin eli verkkokeskustelun vaiheet, verkon erityispiirteet, jotka mahdollistavat verkkorikollisuuden kuten hyväksikäytön, sekä hyväksikäyttäjän ja uhrin vuorovaikutuksen sekvenssien rakentumiset hyväksikäyttöprosessin aikana.

Tutkimuksen pohjalta esitetään sekä suuntaa jatkotutkimukselle että käytännön toimenpiteitä verkkorikollisuuden ja lasten seksuaalisen nettihoukuttelun vähentämiseksi ja muutenkin verkkorikollisuuden tutkimusmetodologian lisäämiseksi.

Avainsanat: kybergrooming, kyberhoukuttelu, seksuaalinen nettihoukuttelu, sisältöanalyysi, kyberrikos, nettirikos, rikosten ehkäisy, seksuaalinen hyväksikäyttö

Author Manja Nikolovska
Faculty of Information Technology
University of Jyväskylä
Finland

Supervisors Professor Mikko Siponen
Faculty of Information Technology
University of Jyväskylä
Finland

Dr. Jan-Henry Stenberg
Head of Division ICT Psychiatry and Psychosocial Treatments
Helsinki University Hospital
Finland

Reviewers Professor Susan Brown
Department of Management Information Systems
University of Arizona
USA

Professor David Maimon
Department of Criminal Justice and Criminology
Georgia State University
USA

Opponent Professor Jean-Louis Van Gelder
Director
Max Planck Institute for Foreign and International Criminal Law
Germany

ACKNOWLEDGEMENTS

The work within these pages is the product of altruistic curiosity, disciplined imagination, and dedication, cultivated through immense support from a network of extraordinary people. Here, I give them my gratitude.

Prof. Mikko Siponen, my principal supervisor and mentor, for his belief in my topic and vigorously bold research vision, skills and drive which have all been an impetus, providing a constant spur of motivation during these four years. Thank you for inspiring the backbone of my research idea, for providing a critical lens that did not constrain creativity of thought, and for your support and guidance in teaching me grounded academic independence. Dr. Jan-Henry Stenberg, my external supervisor, for his courageous expertise and input and his perpetually uplifting attitude to research and life. Thank you for bridging the research with practitioners in the field and providing a psychological anchor in the most challenging aspects of my work. Prof. Volkan Topalli, a co-author and mentor, for our first conversation, which looked like a "think map" of research sparks and ideas. Your background and knowledge provided a voice to the ideas that made the research a whole; thank you! I also thank the Faculty Board for funding my research throughout the years. Dean Pasi Tyrväinen, for having an open door and for supporting my research; thank you. I thank the Finnish Cultural Foundation for a grant that supported the last six months of my research. I thank Prof. Tuure Tuunanen for his support, guidance, and encouragement, especially in my ICIS Doctoral Consortium application. Thank you, for I have learned and gained so much from that experience. I thank the Cyber Security Research Group in our faculty for all the feedback and for fighting "the good fight." Additionally, I thank the external examiners of this work, Prof. Susan Brown and Prof. David Maimon, for their valuable insight and commentary, and Prof. Jean-Louis Van Gelder, my opponent.

I give my utmost gratitude to the Finnish National Bureau of Investigation and the Finnish National Police Board for granting access to data, which was of unique and incredible value for such a research endeavor, and to the Finnish Cyber Intelligence Unit. Sari Sarani, Mikko Veijalainen, Maria Rossi, and Anette Paavilainen, thank you for your dedication and bravery in the front lines of combating online child sexual abuse. I thank you and your teams for your willingness, time, and patience in listening to our ideas and providing us with the necessary material. Without you, this research would not have been possible. I also thank the EC3 Twins Unit, the Swedish National Cyber Crime Centre, Save the Children Finland, and ECPAT Sweden for their interest in and support for the research idea and for collaboratively exploring the possibilities for acquiring data.

Next, I thank Hanna Kinnunen for deciding to rise to the occasion of translating the data. Thank you for all those long hours that we spent in the "vault," translating and transcribing every single line of the data. For all those times that it felt like an impossible and heaviest-to-heart task, thank you for bringing your positive attitude and spirit and remembering the bigger picture.

Hadi Ghanbari for helping me with my systematic literature review in the very early stages of this journey and, from there on, becoming a trusted colleague and friend. Thank you for all the advice, and for believing in our research. Thank you, Hojat Mohammadnazar, for all our discussions on moral development and our sharing of stories on our doctoral studentship endeavors.

Now, I turn to a group of remarkable academics and friends, for our friendship and support became the linchpin in this journey. Juuli Lintula, thank you for being a ray of sunshine in our office every single day, for your passion and virtue in all discussions. Kati Clements, thank you for your strength, for being my rock in unsteady waters, and for that laughter that lights up the room. Naomi Woods, for your inexhaustible compassion, always remembering to check on me, and the most hilarious sense of humor, thank you. Tapio Tammi, for being the "heart of the department", for bringing all the fun and activities, which really contributed to our well-being. Thank you for wearing your smile at all times.

I would also like to thank the following colleagues for all the inspiring talks and a supportive academic structure: Eetu Luoma, Wael Soliman, Johanna Silvennoinen, Markus Salo, Henri Pirkkalainen, Toni Taipalus, Philpp Holtkamp, Cory D. Barker, Ville Isomöttönen, Ari Tuhkala, Tuomas Kari, Arto Ojala. Tiina Lampinen, and Sami Kollanus, thank you for being always helpful and kind. I thank the rest of the members of our faculty for creating an environment that supports academic, professional, and personal growth to the utmost potential.

I am thankful to all my family and friends who believed in me throughout the years. My loving grandparents, Anetta, Christos, Markos, Jana, Milena, Eli, Igor, Amanda, Carolina, Tiina, Niina, Satu, Teppo, and Marjo, thanks for cheering me on. Andrej Angelovski, for being a supportive partner. I am thankful for our growth together, for every day, I learn from you and your love of curiosity. Thank you for showing me a way to love STATA and for being my shelter this year.

My warmest gratitude goes to my parents. My mother Margarita, for her fierce energy that has been the "light" for me and my family. My father Tihomir, for being the perennial role model and for sparking my drive by once saying: "in case you could not save the world… if you ignited a positive change, even in one person's life, you have accomplished your mission." Thank you both for setting the sky as my limit!

I dedicate this work to my amazing sister, who is ten years younger, for her generation has inspired the fight in me to try and make the Internet a better place. My final thanks goes to you, Dona, for I will never stop trying.

Jyväskylä, 18.11.2019
Manja Nikolovska

FIGURES

TABLES

CONTENTS

LIST OF ABBREVIATIONS

CGOC	Cyber grooming of children
CG	Cyber grooming
CSAM	Child sexual abuse material
SGCAM	Self-generated child abuse material
SLRA	Systematic literature review and analysis
GA	Gap analysis
CAM	Requests for/or creation, exchange, and distribution of child abusive material

1 INTRODUCTION

Internet use has revolutionized how people communicate and transact business. It has also been a seedbed for deviant and criminal behaviors, including, cyber harassment, cyber stalking, cyber bullying, and cyber grooming, now being examined in the information systems (IS) discipline. Consequently, editorials in *MIS Quarterly* (Lee; 2015; Mahmood et al., 2010) have highlighted the need to examine the most serious cybercrime offenses.

The cyber grooming of children, a form of online child sexual abuse, is one of the most vivid examples of a physical-world-based abuse that becomes more pernicious when perpetrated in cyberspace. Its prevalence and perpetration in the online world are sufficiently different in scope and execution from what we know of abuse in the physical world to warrant reconceptualization and theoretical innovation. One of the many characteristics that make cyber grooming dangerous is that a child who is safely at home can be targeted from anywhere in the world. For example, an adult offender befriended an 11-year old through Facebook, after acquiring several friends in common with the victim and representing himself as a peer (Hannah, 2017). Even though the victim had been educated not to befriend strangers online, the existence of mutual friends meant that she was disinclined from considering the offender as a stranger. After exchanging jokes and emojis, the offender turned on his Facebook webcam during the chat and exposed himself while masturbating in view of the 11-year old. Most online abuse consists of chat conversations within a sexual context, sharing photos or videos containing sexual content, virtual sex via webcam, and even live streaming of the child self-inflicting abuse. In the example cited above, after the victim rejected further webcam contact, the offender continued sending her obscene, derogatory, and sexually abusive messages. The victim waited more than a year before disclosing the incident to her parents because she felt ashamed and responsible for what had happened to her. In many cases, victims are trapped in a cycle of abuse by offenders who blackmail them, threatening to expose the material already exchanged. Victims experience grave psychological consequences, sometimes leading to suicide (Murumaa-Mengel, 2015), while

offenders remain in cyberspace, with the ability to abuse multiple victims simultaneously.

A systematic review of the literature on cyber grooming (n = 135) identified four major gaps: 1) a lack of cyber-specific explanations; 2) an overreliance on traditional theoretical formulations; 3) an overreliance on static models of behavior; and 4) inadequate process modelling. The previous literature is also silent on empirically addressing the role of cyber-specific behavioral variables, as expressed by the offender and victim, in the dynamic cyber-grooming process.

As a response to the major shortcomings in the literature, this dissertation offers a novel way of studying cybercrimes, specifically the cyber grooming of children (CGOC)[1] as a form of sexual abuse that takes place in the online world. It strives to shift the perspective from the prevailing view of the Internet—as a tool or means by which to perpetrate cyber grooming—toward viewing it as an engine that might guide and shape behavioral paths around a phenomenon that we can track and record. Its key assumption is that while previous theories and models on cyber grooming identify the proper variables of interest, these variables are built on physical-world-based assumptions about human cognition, behavior, and social structure, which are radically altered in cyberspace (see Kellerman, 2014, 2016). Since cybercrimes occur in a "landscape" where traditional notions of time and space are governed by a different set of rules and parameters, many of the predictions about cybercrime derived from traditional models will be insufficient as tools for explanation, prediction, and efficient prevention.

For this purpose, the dissertation conceptualizes cyber affordances as cyber-specific conceptual variables and explores how the offender and victim might be using such affordances during the occurrence of the cyber-grooming process, i.e., in real time and real life. The empirical study presents results from chat-log transcript data obtained through the Finnish National Bureau of Investigation (NBI). The study employs a mixed-methods approach. First, qualitative content analysis is applied to the chat messages from the NBI data. Second, since the data offer a time stamp of each message in order to increase the qualitative explanatory power, the study constructs panel data using the time stamp of each message and its corresponding code, assigned by the qualitative content analysis. Lastly, the study applies descriptive and regression analysis of the qualitative codes.

The findings present the use of the cyber affordances discovered in the chats, the offender's and victim's paths in the cyber-grooming process and most

[1] In this dissertation, I use the term "cyber grooming of children" (CGOC) as a catch-all phrase to describe and encompass various forms of adult victimization of children, perpetrated on the Internet, including: "solicitation of children for sexual purposes" (as defined in Article 23, Lanzarote Convention, 2007, 2011: EU Directive 2011/93, and the 2015 "Opinion on Article 23 of the Lanzarote Convention and Its Explanatory Note"); "online grooming for sexual purposes"; "online sexual enticement of children"; and "sexual extortion of children as result of grooming" (see Section H3, p. 49 ,in Terminology and Semantics Interagency Working Group on Sexual Exploitation of Children. Terminology guidelines for the protection of children from sexual exploitation and sexual abuse. ECPAT International, 2016).

critical incidents occurring in the chat. The interpretation of the findings produces practical and theoretical implications for both academia and practitioners.

1.1 Phenomenon background

Child sexual abuse is described as "…the involvement of a child in sexual activity that he or she does not fully comprehend, is unable to give informed consent to, or for which the child is not developmentally prepared and cannot give consent, or that violates the laws or social taboos of society" (UNODC, 2014, p.7; WHO, 2003, p.75). While contact abuse involves physical interactions with a child, including penetration, non-contact abuse includes grooming, exploitation, and persuading children to perform sexual acts over the Internet (NSPCC, 2018a). "Grooming/online grooming refers to the process of establishing/building a relationship with a child either in person or through the use of the Internet or other digital technologies to facilitate either online or offline sexual contact with that person" (ECPAT, 2016, p.51). "Relationship building" is achieved through the use of social engineering techniques (see Mann, 2017; Stewart & Dawson, 2018) that involve connecting with, influencing, and psychologically nurturing the child for the purpose of abuse. This may take the form of offering advice or empathy, buying gifts, giving the child attention, or using their financial resources, professional position, or reputation to benefit the child, including taking them on trips, outings, or holidays (see Deitz, 2018; Lanning, 2018). These activities are all aimed at ongoing and/or subsequent exploitation of the child for sexual purposes.

Offline child sex grooming occurs in the physical environment where time, location, and physical appearance present constraints on sexual predators (e.g., limits on the number of potential victims, ease of communication, the ability to misrepresent one's identity, etc.). Further, in the physical world, 90% of offline child grooming involves abuse by someone familiar to the child (e.g., family members or close friends of the family; see Radford et al., 2011). As we will note below, there are a variety of technology-based advantages to engaging in grooming over the Internet, thereby fueling the increase of the practice. The practice differs from physical-world grooming, in that, it is almost always perpetrated by strangers (EPCAT, 2016). Online, offenders are unrestrained by physical distance or appearance and are able to take advantage of the contextual offense-related affordances of the internet, magnifying the effectiveness of social engineering techniques and expanding their reach, all with the click of a mouse. This increases children's online vulnerability to many more predators, who may reside anywhere in the world. Unsurprisingly, therefore, in one in four reports from almost 6,000 cyber-grooming cases, the offender had multiple victims (National Center for Missing and Exploited Children [NCMEC], 2017).

In the US, the CyberTipline operated by the NCMEC (2017) received over 10.2 million reports of suspected child sexual exploitation in 2017 alone,

including online enticement or CGOC. In 2018, the FBI arrested more than 2,300 online child sexual offenders, while the Internet Crimes Against Children taskforce investigated over 25,200 complaints of technology-facilitated crimes against children (US Department of Justice, 2018). The UK saw a 50% increase in online grooming cases between 2017 and 2018, with 3,000 new cases recorded (National Society for the Prevention of Cruelty to Children [NSPCC], 2018b). In 70% of these cases, the grooming was performed through Facebook, Snapchat, or Instagram. The nature of Internet communications and the desire of online predators to maintain anonymity are just two reasons why CGOC is underreported and thereby implicated in the "dark figure" of crime (Biderman & Reiss, 1967).

Evidence of the prevalence of online child sexual abuse can also be observed in the proliferation of child sexual abuse material (CSAM). The latest Internet Organized Crime Threat Assessment (IOCTA, 2018) report by Europol identified online child sexual exploitation as one of the fastest growing modes of cybercrime, with a significant growth in the detected of online CSAM. In 2017, the Canadian Center for Child Protection processed over 230 million web pages, which detected 5.1 million unique pages hosting over 40,000 unique images of child sexual abuse (IOCTA, 2018). Also in 2017, the Internet Watch Foundation (IWF) identified a record 80,000 instances of online child sexual abuse imagery (IWF, 2017). The majority of the identified child sexual abuse web pages (57,335) were hosted in Europe (60%), and 37% were identified as being hosted in North America (IWF, 2016). Overall, 92% of all child sexual abuse URLs identified globally by the IWF are hosted in five countries: the Netherlands, the United States, Canada, France, and the Russian Federation (listed by most to fewest URLs) (IWF, 2016).

One source of this growth is the continuous creation of self-generated child abuse material (SGCAM; i.e., naked/provocative selfies/videos taken by the children themselves). This term refers to a scenario in which the child is alone, or with other children, and is persuaded or "groomed" into taking images or videos of themselves engaged in sexual activities and then sharing this content, often with someone they trust (IWF, 2018). One in three instances of reported online CSAM is categorized as self-produced, 96% of which depicts a child in their home environment (IWF, 2018). Ninety-eight percent of the material features children aged 13 and below, with the youngest victim being just three years old (IWF, 2018).

Offenders can procure such material in a variety of ways. In many cases, SGCAM are voluntarily shared between child peers via sexting, distribution on social networks, or through mundane or viral sharing (e.g., revenge porn). It is often acquired through the cyber grooming and sexual extortion of minors by adults (IOCTA, 2017; IWF, 2018, see also Acar, 2016; Chiang & Grant, 2018). The IWF (2018) has warned that any legitimate Internet communication tool that offers live streaming represents a potential access, retention, and distribution platform for offenders. Social networking sites, such as Facebook, SnapChat, ImGur, and Instagram, provide ideal settings for interacting with younger

victims. Offenders can use them to create and delete authentic-looking fraudulent profiles and falsify their geographical locations, all with greater ease and frequency than would be possible in the use of face-to-face communication.

These and a host of other emerging communication platforms essentially eliminate physical distance between victims and predators for the purpose of crime, while simultaneously enhancing barriers to detection and interdiction. Internet technologies also increase the scope and scale of victimization by giving child sex predators access to a global victim pool (see, e.g., Chua et al., 2007; Grazioli & Järvenpää, 2000). Offenders can take advantage of this to operate with some level of impunity because law enforcement and prosecutorial recourse are limited by geographically determined jurisdictional boundaries. Tracing, investigating, and prosecuting online sex offenders entail significant coordination and cooperation involving victims, law enforcement, and the IT businesses whose platforms are exploited for offending. These limitations are particularly acute when predation occurs internationally (see Button et al., 2014), where jurisdictional conflicts are more likely and more difficult to resolve. In addition, it is also important to mention crime as-service, in which criminals acquire photo or video material of children and sell it on the anonymous dark web in exchange for anonymous cryptocurrencies (e.g., bitcoin). Consequently, the Internet offers a low-threat setting for individuals to engage in crime, with significant implications for deterrence and control, particularly of cyber grooming.

In terms of the future outlook, we know that network connectivity spreads and improves with each passing day, allowing live broadcasts and live streaming from nearly anywhere and at any time. Modern smartphones, tablets, and personal computers already have high-quality cameras and will soon be equipped with 5G network.

All this considered, it is not an exaggeration to state that although sexual predation has a long and sordid history going back to prehistoric times (DeMause, 1997; Olafson et al., 1993; Radbill, 1968), this phenomenon has also been revolutionized by the advent of online social communication platforms, which have vastly increased the vulnerability of children and the ease with which offenders can target and interact with them (Wolak et al., 2009; Wurtele et al., 2016). The scenario of a predator preying on a child in a playground is shifting into one in which that "playground" is now in the child's pocket or bedroom.

1.2 Scope of the dissertation

This dissertation introduces a novel way of studying cybercrimes, such as cyber grooming. It strives to shift the perspective from the prevailing view of the Internet—as a tool or means through which to perpetrate cyber grooming—toward viewing it as an engine that might guide and shape the behavioral paths around a phenomenon that we can track and record.

By studying cyber grooming in this context, this dissertation introduces concepts such as *cyber affordances and cyber sub-affordances* by identifying the behavioral characteristics manifested in chat communicative environments. It strives to provide knowledge on *cyber behavior hygiene and etiquette* as a means to educating young generations to come. By shifting the research focus from studying the transfer of personality traits from the physical world to the online world (very often in dissonance) to developing personality traits deriving from cyber-exclusive opportunities, such as anonymity and fantasy, we are transcending toward cyber-exclusive developmental paths and new *cyber* behavioral exploration frontiers.

1.3 Research objectives

The research objectives of this dissertation are threefold: first, to identify the gaps in the existing literature on CGOC; second, to propose a novel "cyber-specific" conceptual model on CGOC; and third, to empirically demonstrate the potential of this model by applying it to CGOC chat logs of real-life abuse cases.

The main sections of the dissertation are structured as follows: In Section 2, the systematic literature review on cyber grooming is presented, and four major research gaps are identified. First, the theories used in the existing research to explain the phenomenon were not meant for cyber grooming but for other forms of crime. Most of them were developed for crimes in the physical world and did not account for the characteristics of the Internet in terms of their development or application. Second, most existing studies focus on static factors and fixed relationships that explain or predict the behavior behind the act of cyber grooming (e.g., pedophilia causes cyber grooming). This means that the models cannot account for changes in the relationship between the static factors and cyber grooming (e.g., the offender is not a pedophile but engages in sexual grooming for other purposes, such as sextortion). Third, other study streams focus on the steps or process of how the act of cyber grooming is committed, for example, stage models of how the act of the abuse begins, progresses, and ends or process models with fixed relationships between the different constituents of the act. In general, the usefulness of stage models rests on how well the victim's or perpetrator's actual path matches the stages. Unfortunately, offenders and victims tend to shift or skip stages (Elliot, 2015; Williams et al., 2013), or they may use more than one stage simultaneously, which cannot be captured in step-by-step models. None of these models have considered the victim's input in real time and how this input may affect the offender's path in the suggested process. Last, the use of Internet characteristics between the offender and victim (which might distort the static predictors and the fixed-stage progression) during the cyber-grooming abuse process has not been explored.

Based on these gaps, Section 3 of this dissertation proposes a Cyber affordance model of cyber grooming that strives to study CGOC through an exploration of cyber-specific behavioral affordance and how the offender and

victim utilize these affordances during the abuse process. This model conceptualizes cyber behavior affordances based on online disinhibition. The model proposes a way in which to record the use of these cyber affordances by the offender and victim during the abuse process in order to determine cyber motives among offenders and cyber vulnerabilities among victims. It also seeks to demonstrate how the use of these characteristics can guide the paths of the offender and victim throughout the abuse process.

In Section 4, I present the empirical study: the data collection, methods employed, and the findings of the empirical test of the conceptual model. For the purpose of this research, the data collection was performed on chat-log transcripts of real-life cases of cyber grooming. The data were collected from the Finnish NBI by gaining access to police data through a form of security clearance for myself and my two supervisors. In Section 5, I discuss the results, followed by the theoretical and practical contributions in Section 6. In Section 7, I present my concluding remarks.

2 SYSTEMATIC LITERATURE REVIEW

This research first employed a systematic literature review and analysis (SLRA) of the existing research on cyber grooming (n = 135) (Appendix 1). The SLRA identified two broad gaps in the CGOC research knowledge base: 1) a lack of cyber-specific theorizing and model development and 2) a lack of conceptualization regarding causal orientations (situational versus dispositional) for CGOC offending. The purpose of the SLRA was to identify strengths and gaps in the extant literature on CGOC for the purpose of model formulation. SLRAs are endorsed in the information systems literature by Okoli and Schabram (2010) and Webster and Watson (2002) and in the criminological literature by Groff, Johnson, and Thornton (2018). In both cases, researchers have established principles for conducting SLRAs to "…take stock of the literature to date with the aim of informing and improving future research…" (Groff et al., 2018, p. 4) as well as to "…summarize existing evidence, identify gaps in current research and provide a framework for positioning research endeavors" (Okoli & Schabram, 2010, p. 3).

The SLRA is an empirically based exercise that identifies the appropriate population of studies focused on CGOC in order to develop a conceptual platform from which to build a model that responds to each gap identified in the research. This is referred to as a gap analysis (GA), an approach prevalent in the marketing and management sciences, as well as in systems engineering, where it is employed to study the current state of a system (such as a business, intervention, organization, or research area) and where it may need to go in the future. In the social sciences, GA can help develop new theories or models by applying an empirical process (e.g., the SLRA) to identify weaknesses or gaps in a research area (in this case, child grooming as an online phenomenon; see Kumar, 2005; Wotela, 2017). This allows us to incorporate or redefine traditional theoretical concepts and add new ones so as to accommodate the unique impact of online environments into our understanding of (cyber) grooming.

I now proceed to describe the process of conducting the review, according to eight principles laid out by Okoli and Schabram (2010):

1. **Identify the goal of the literature review**

   The SLRA assesses the current understanding of why and how CGOC is performed as a cyber-exclusive offense. My goal was not to assess child abuse research in general, child abuse performed in the physical world, or online/offline child abuse material/pornography research.

2. **Implement a specific protocol and training**

   To increase the comprehensiveness of the selected literature and the replicability of the review, I designed a protocol outlining the initial scanning sequences for selecting the literature, the inclusion and exclusion criteria, and the principles of the content analysis of the included papers that would target the goals identified in the purpose of the review (see below).

3. **Literature search**

   In the first step of the literature review, I searched and scanned the following repositories: Springer, Tandfonline, Wiley Online Library, SagePubs Online, AIESEL.AISNEt, Elesevier, Communications of the ACM, altogether 3,911 journal repositories. In keeping with procedures established in the library sciences (see, e.g., Papaioannou, 2010), the initial scanning applied keyword sequences composed of the following word groups derived from the previously discussed specified definition of CGOC:

   cyber OR online OR Internet

   AND

   grooming OR sexual OR sex OR abuse OR offence OR offending OR offender OR victimization OR solicitation

   AND

   child OR children OR youth OR young OR minors

4. **Practical screen**

   The practical screen identifies the inclusion criteria to be applied to the population of eligible papers derived from the repository scan. It also establishes the rules governing which papers are to be excluded without further analysis (Okoli & Schabram, 2010). For this purpose, I employed these rules in the initial scanning of the identified works and the subsequent follow-up scraping (see Munzert et al., 2014) of titles and abstracts across the entirety of the previously listed repositories.[2] The following inclusion criteria were identified:

   a. Internet-specific aspects of grooming or child sexual abuse. To capture cyber behaviors exclusively, and exclude research focusing

[2] The initial scanning was conducted between 2015 and 2016. The papers included were published before 2016. This time frame was determined as a natural byproduct of the point at which the systematic literature review was conducted.

on physical-world- or traditional child abuse, I excluded papers that did not contain the words represented in Group A below in their title and abstract:

$$\text{Group A} = (\text{“Cyber”}=A_1)\pm(\text{“Online”}=A_2)\pm(\text{“Internet”}=A_3) \rightarrow \text{Group } A_{(1)\pm(2)\pm(3)}$$

b. CGOC concept-related processes. The search parameters were limited based on terms related to CGOC and focused on research highlighting the concept (and term) of “grooming,” such as cyber/online/Internet “grooming” of children. Thus, the term grooming is not comprehensively accepted as unique and exclusive to capturing CGOC as the definition used for the purpose of the SRLA. As such, besides the term “grooming,” I added (“sexual” or “sex”) parameter identifiers as terms that would limit and focus the phenomenon strictly on sexual abuse, while abandoning orthogonal phenomena such as (cyberbullying/cyberstalking/harassment). I also added “Abuse”; “Offence/Offending”; “Victimization”; or “Solicitation(s).” Through this criterion, I excluded papers that did not contain the words represented in Group B below in their title and abstract:

$$\text{Group B} = (\text{“Grooming”}=B_1) \pm (\text{“Sexual/Sex”}= B_2) \pm (\text{“Abuse”}= B_3)\pm(\text{“Offence/Offending/Offenders=} B_4) \pm (\text{“Victimization”}= B_5) \pm (\text{“Solicitation(s)”}= B_6) \rightarrow \text{Group } \mathrm{B}_{(1)\pm(2)\pm(3)\pm(4)\pm(5)\pm(6)}$$

c. The third inclusion criterion limited the victimization scope to children. Here, I omitted articles on the cyber sexual victimization of young adults (age between 18–25) or adults (over 25). Thus, the third inclusion criterion identified papers that specified in their title and abstract the wording represented in Group C:

$$\text{Group C} = (\text{“Child/Children”}= \mathrm{C}_1) \pm (\text{“Youth/Young”}= \mathrm{C}_2) \pm (\text{“Minors”}= \mathrm{C}_3) \rightarrow \text{Group } \mathrm{C}_{(1)\pm(2)\pm(3)}$$

A paper was included (In) in this literature review for further content analysis if it satisfied one parameter from Group A, one from Group B, and one from Group C, without its inclusion being tied to the order of appearance of the group words:

$$\mathrm{A}_{(1)\pm(2)\pm(3)} + \mathrm{B}_{(1)\pm(2)\pm(3)\pm(4)\pm(5)\pm(6)}\mathrm{C}_{(1)\pm(2)\pm(3)} \rightarrow \text{Group A + Group B + Group C= (In)}$$

For example, the paper A Linguistic Analysis of Grooming Strategies of Online Child Sex Offenders: Implications for our Understanding of Predatory Sexual Behavior in an Increasingly Computer-mediated World (Black et al., 2015) was included on the basis of the following expression:

$$\text{In}= B_1 + A_2 + C_1 + B_2 + B_4 \rightarrow A_2 + B_{1+2+4} + C_1 \rightarrow \text{Group A} + \text{Group B} + \text{Group C}$$

There are exceptions to these rules of inclusion. First, so as not to exclude papers that treated the "cyber/online/Internet grooming" category as synonymous with or indicative of online child sexual abuse (e.g., a paper titled How Technology Can Mitigate and Counteract Cyber-stalking and Online Grooming), I applied additional keyword content analysis of the paper using the Group C criterion. If the additional keyword content analysis identified that the paper did indeed address OGOC, it was included in the next phase of the review. Second, if the selected paper's title and abstract captured "cyber sexual offending" or "cyber sexual victimization" without specifying a specific type of offense, I performed an additional keyword content analysis to evaluate whether it focused on grooming/solicitation and whether it was targeted toward children (keyword content analysis in relation to Group A and Group C). If this process identified that the paper discussed cyber sexual offending/victimization of children through grooming/solicitation, it was included in the next phase of the SLA.

5. Quality appraisal

The quality appraisal sets out the criteria for evaluating papers that do not satisfy the purpose of the review and, therefore, ought to be excluded (Okoli & Schabram, 2010). In this research, I focused on CGOC as a vivid example of how a specific type of criminal behavior changes when performed in the online world. For two reasons, I resisted including other deviant cyber phenomena involving children or studies focusing specifically on online CSAM, pornography, bullying, harassment, extortion, etc. For the exclusion process to be sufficiently robust as a descriptive and predictive tool, it is important to specify the phenomenon in question and limit its scope. A strictly identified categorization eases the GA and subsequent theory or model construction. This is particularly important when dealing with cybercrimes, which tend to be multi-faceted, as they often co-occur with other offenses within incidents rather than as one-off crimes.

Additionally, cyber phenomena can overlap. For example, while producing and distributing CAM or engaging in sextortion can be achieved through the grooming process, they may also represent stand-alone phenomena. Therefore, to remain in line with the scope of the cyber-grooming phenomena, I excluded the papers whose title and abstract signaled that they specifically studied child pornography or child abuse material, child exploitation material, bullying, harassment, and extortion, as represented in Group D:

$$\text{Group D} = (\text{"Pornography/porn/pornographic"} = D_1) \pm (\text{"Child abuse material/CAM"} = D_2) \pm (\text{"Child exploitation material"} = D_3) \pm (\text{"Bulling"} = D_4) \pm (\text{"Harassment"} = D_5) \pm (\text{"Extortion"} = D_6) \rightarrow \text{Group D}_{(1)\pm(2)\pm(3)\pm(4)\pm(5)\pm(6)}$$

At the same time, while I included works referring to such side phenomena as part of, or resulting from, the cyber-grooming process, I did not exclude papers whose title and abstract contained words from Group D in relation to cyber grooming/solicitation or papers, which following further content analysis, signaled the inclusion of Group D as a result of the grooming process.

6. Data extraction

The initial broad scan produced 96,686 papers. Applying steps 4 and 5 above resulted in 135 studies that were viable for data extraction based on the purpose of the review. In light of this, the exploratory mandate was to evaluate:

a. how many papers considered any "cyber" unit of analysis/constructs to be related to cyber grooming;
b. the theoretical approach of each paper (testing, building, referencing, or not using theories for cyber grooming);
c. the type of contribution of the paper (offender-based vs. victim-based);
d. enactment-based (i.e., how cyber grooming is performed), for example, process/stage models; and finally,
e. whether the papers were empirical or conceptual.

I used a qualitative approach to assess the data extraction (see Denyer & Tranfield, 2006), using a reference management software[3] (see Bandara et al., 2011). For the Internet and empirical/conceptual category, I used binary coding (e.g., a paper either considers or does not consider Internet constructs, or the paper is either empirical or conceptual, etc.). For the theoretical assessment, I used four exclusive codes (a paper tests, builds, references, or does not use any theories of cyber grooming). To assess a paper's contribution, I used an inclusive tagging system for motivation, enactment of CGOC, and offender- and victim-based studies. These categories are not mutually exclusive by design, as I sought to incorporate papers with multiple, overlapping contributions.

7. Synthesis and descriptive overview of studies

The previously laid-out scheme was used to develop categories representing the occurrence of papers in the database by code (as presented in Appendix 1), whose results are presented in Figure 1 below. First, in studying cyber grooming, a majority of the papers (n = 117) did not include Internet-specific attributes in their unit of analysis or conceptual constructs. Only 18 papers considered some aspect or attribute of the Internet. This provided the first indication of the need for a cyberspace-relevant conceptualization and model building. Second, most of the papers did not employ a specific theoretical lens (n = 80). Those that did reference more than one theory to support or build their argument (n

[3] Mendelay Desktop - Version 1.19.3 © 2008-2018 Mendelay Ltd.

= 33) indicated that theory formulation was, at best, a secondary consideration; 14 papers engaged in theory building, while 8 carried out theory testing. Third, most of the papers concentrated on causation relating to CGOC (n = 61). Of those, 46 studies concentrated on offender motivation and 19 on victim vulnerabilities. Fourth, papers tackling the enactment of child grooming (n = 50) largely focused on how offenders perform abuse (n = 43), while a small portion considered victim responses without consideration of the offender (n = 15). A majority of the papers were empirical (n = 86), while the rest were conceptual (n = 49).

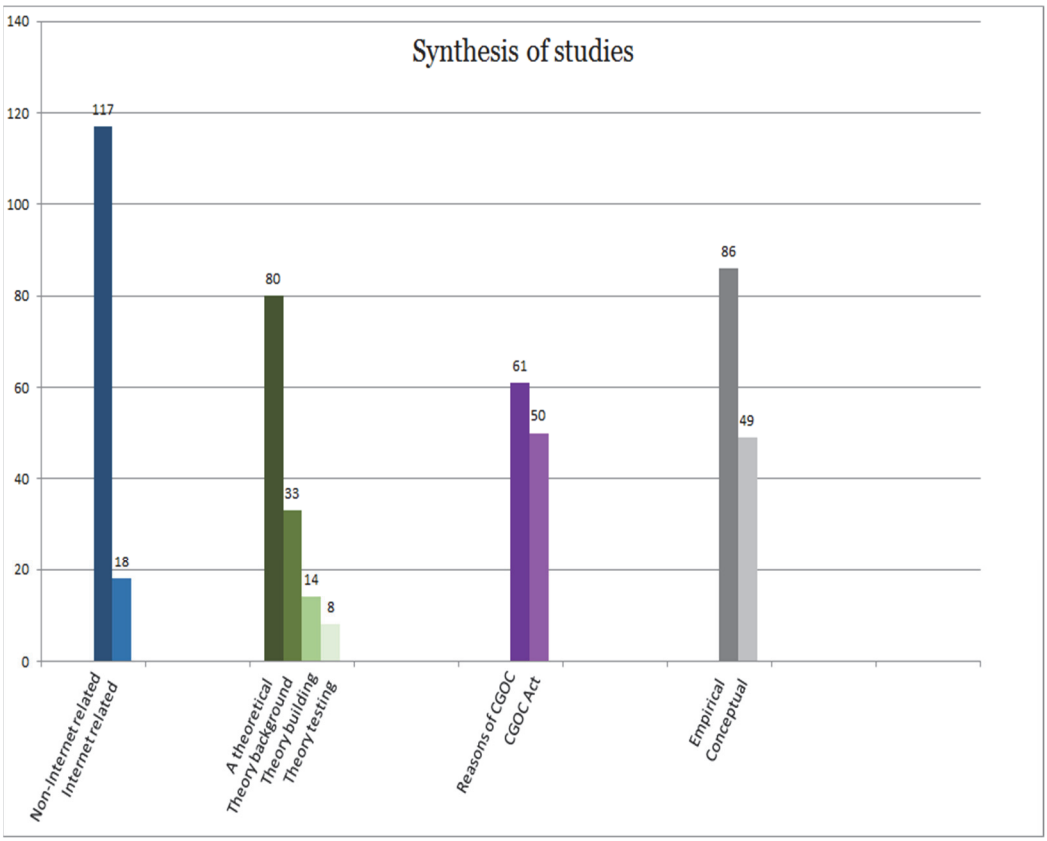


Figure 1: Systematic literature review: Synthesis of studies

8. Empirical review: Gap identification and model formulation

Once the database of papers was established and coded, the resulting papers were assessed for weaknesses or lacunae in the current state of research on CGOC as a phenomenon driven by the Internet environment. This is in keeping Epstein's (2006, 2008; Epstein & Axtell, 1996) generative approach mentioned previously. Identifying gaps through this process is inductive because it surveys the extant knowledge regarding a phenomenon without postulating or predicting specific a priori relationships between concepts that may underlie it. The relationships are gleaned from the analysis.

The overarching finding was that no empirical paper adequately incorporated the role of internet-specific behaviors connecting offender

> motivation and victim vulnerability during the cyber-grooming process. Further, the extant theorizing about the etiology of CGOC is over-reliant on traditional models of criminality, and it does not incorporate the Internet or online environments as a contextualizing or casual element. Research on CGOC tends to focus on identifying "groomers" as a distinct group and fails to integrate many of the online situational dynamics of their behavior, which is important for prediction and prevention. It also fails to incorporate the victim's input or process into the CGOC models. Assuming that child grooming does not operate online in the same way that it does in the physical world, this represents a major weakness in our understanding of CGOC. The synthesis of the studies revealed four major gap categories: lack of cyber specificity; overreliance on traditional theories of crime; overreliance on static models of behavior; and inadequate process modeling.

In the next section, I follow Webster and Watson's (2002) approach to theory appraisal of a literature analysis, assessing each gap by "highlighting the discrepancy between what we know and what we need to know" (p. 19). I then suggest the conceptual model as "an alert to other scholars as opportunities for key contributions" (p. 19).

2.1 Lack of cyber specificity

The cyber environment is stripped of many of the physical-world features to which humans anchor in deciding how to think and behave. Interacting with others online may take place without having to consider physical appearance, knock on doors, physical closeness, maintaining eye contact, or attenuating one's voice, among other examples. These kinds of mundane precursors to social interaction can be critical to proper social functioning in the physical world. Their absence online can lead to errors in social information processing and aberrant behavior. Consequently, technology-enabled environments can alter decision-making behavior and human perception (see Gutzwiller et al., 2016; Wallace, 2015). For example, online chat forums create artificially anonymous social settings, which have been found to increase stereotyping (Fox, et al., 2015; Ivory et al., 2014), racism (Keum & Miller, 2018; Ronkin & Karn, 1999; Steinfeldt et al., 2010), and aggression (see Lapidot-Lefler & Barak, 2012; Moore, et al., 2012; Zimmerman & Ybarra, 2016). In addition, a great many social communication platforms govern human interactions through algorithms and machine-learning processes that privilege efficiency over social comportment.

Suler (2004) introduced the Internet disinhibition effect, which states that the interaction of six Internet attributes encourages users to behave differently in the online world than they do in the "real" (i.e., "offline") world. These are *dissociative anonymity* (the ability for the user to "play" with identity), *invisibility* (the ability to visit "places" or do things without facing social judgement or

control), *asynchronicity* (the ability to avoid immediate reaction), *solipsistic introjection* (which occurs when individuals project/imagine a voice or image onto another person with whom they are interacting), *dissociative imagination* (the state of mind wherein users view their online presence as detached from real life), and the *minimization of status and authority* (feeling at ease about expressing behaviors that they would not express in the physical world, perhaps due to mechanisms of social and law enforcement control). According to Suler (2004),

> "The disinhibition effect can then be understood as the person shifting, while online, to an intrapsychic constellation that may be, in varying degrees, dissociated from the in-person constellation, with inhibiting guilt, anxiety, and related effects as features of the in-person self but not as part of that online self." (Suler, 2004, p. 325)

Moreover, there is a dearth of CGOC-related research that measures or includes cyber-specific causal or conditioning variables—attributes or characteristics that could potentially impact the behavior of offenders and victims. Cyber-specific variables can be seen as predictors and descriptors of human behavior, which incorporate or rely on the unique nature of online environments to have their effect on perception and behavior, particularly when they are seen to influence and alter the foundations of human interaction. More than 85% of the studies in the review herein included no cyber-specific measures or concepts. For the remainder, their inclusion of online/cyber/Internet-based variables was limited. For example, Kerstens and Stol (2014) incorporated a measurement of online disinhibition using a short 7-item scale for children, based on Suler (2004) and Schouten, Valkenburg, and Peter (2007). The scale was designed to assess the extent to which children received online sexual requests and produced CAM. Quayle et al. (2014) catalogued Internet-specific use by offenders seeking sexual interactions with children. They found that groomers employed characteristics of online environments and social platforms to create private and safe spaces (for themselves) within which to offend, e.g., encrypted private chat rooms and the like. Their grounded approach identified patterns in offenders' interviews that revealed how they chose technologies, changed identities, selected targets, used images, and practiced Internet-specific social engineering techniques to victimize children.

Internet use has been pathologized in the psychological and psychiatric literature (for work on Internet addiction or pathological Internet use, see, e.g., Shapira et al., 2000; Young, 1998). For example, in the same way one can become physically dependent to alcohol or drugs, Internet users can experience intense preoccupation with using the Internet (dependence on time spent online, checking social media, Internet shopping, among other examples) (Chou et al., 2005; Treurer, Fabian, & Furedi, 2001; Yellowlees & Marks, 2007; Young, 1998). Diagnostic criteria for identifying such disorders incorporate technology-specific characteristics of cyberspace, online social platforms, and Internet communication modes (for a discussion of the criteria included in diagnoses, see

Beard, 2005; for a recent assessment of diagnostic criteria, see Poli, 2017). The literature analysis revealed that this approach has been applied in limited fashion to assess the specific role of online technology on CGOC offending and victimization. The integration of cyber-specific constructs makes sense, as Internet addiction disorders have been found to evidence high comorbidity with other mental disorders (e.g., depression, social anxiety disorders, impulse control disorders; see Hawi, 2012) that are themselves directly or indirectly related to pedophilia and CGOC (see also Block, 2008; Elliott, 2016; Wachs et al., 2018). Two papers integrated diagnostic categories related to Internet pathologies into their offender interviews. Quayle and Taylor (2003) developed the model of problematic Internet use for people with a sexual interest in children, which included such Internet-dependent concepts as online anonymity and disinhibition, accessibility of fantasy content, Internet influences on cognitive functioning, and problematic interactions between child-based attraction and Internet use (see also, Quayle, Holland, & Linehan 2000).

The above-mentioned papers that integrated internet-specific attributes represent preliminary but rudimentary attempts at formulating a more systematic integration of cyber variables into research on CGOC—moving toward the development of models of cyber-influenced cognition and behavior.. Such papers were in the minority and did not fully or systematically develop and integrate cyber factors as a key goal of research, thus affirming the existence of a gap. This also speaks to the difficulty involved in conceptualizing a general, unified model or idea of how we should measure cyber characteristics and constructs in such phenomena. Properly typologizing and standardizing such concepts would lay the groundwork for the future development of cyber-specific theories of CGOC and other types of online offending.

2.2 Overreliance on traditional theoretical formulations

The majority of work on CGOC does not reference theory at all. The studies that do rely heavily on established criminological, psychological, and social theories of crime. Of the papers included in the literature analysis, 40% referenced a theoretical explanation of the phenomenon. Most often, this included theories borrowed from other disciplines, which were originally formulated for other forms of crime in the physical world.

The most prevalent theoretical approaches (in order of most common usage) include:

Routine activities theory (RAT), a situational crime prevention theory by Cohen and Felson (1979), cited in Agustina (2015), Cohen-Almagor (2013), Durkin (2009), Hillman et al. (2014), Marcum et al. (2010), Mitchell et al. (2007), Navarro and Jasinski (2015), Quayle and Taylor (2003), and Wells and Mitchell (2008).

Pathways model of child sexual abuse, a psychological pathways model by Ward and Siegert (2002), cited in Craven, Brown, and Gilchrist (2006), McManus et al. (2016), Wall, Pearce, and McGuire (2011), Winder and Gough (2010), Surjadi et al. (2010), Palasinski (2012), Kloess, Beech, and Harkins (2014), and Middleton et al. (2007);

Theory of luring communication, or communicative entrapment theory, by Olson et al. (2007), cited in Whittle et al. (2013), Miah et al (2015), McManus et al. (2016), Cano, Fernandez, and Alani (2014), Vartapetiance and Gillam (2014), McGhee et al. (2011), and Michalopoulos, Mavridis, and Jankovic (2014).

The extent to which such theories—developed for "traditional" crime occurring in the physical world—can provide accurate explanations of emerging offenses unencumbered by the limitations of physical space, such as cyber grooming, is open to question. To illustrate this, I cite the example of RAT, which was first developed in the 1970s to explain robberies and is the crime theory most commonly applied to cyber grooming. According to RAT, for a crime to occur, three conditions must converge in time and space: 1) the presence of a suitable target; 2) the presence of a motivated offender; and 3) the lack of a capable guardian to prevent the crime. These assumptions have been modified in an attempt to accommodate the cyber-grooming phenomenon. For example, in the literature reviewed, researchers extended or adapted the assumptions of RAT to the online context. One study measured the degree of exposure to motivated offenders, using the number of hours the victim spent online (Marcum et al., 2010). Likewise, a victim's suitability as a target was measured by how much personal information he or she had disclosed online. Guardianship, or the lack thereof, was measured by the use or non-use of protective software.

Now, consider a situation in which an 11-year-old child is using Chatroulette, an online chat website that pairs random users for webcam-based conversations, and is subjected to indecent exposure on the webcam stream of a 50-year old located on the other side of the world. Later, the same predator initiates a chat conversation and manipulates the child into further webcam abuse, obtaining naked selfies/videos that are then used to extort the child. It becomes much more difficult to fit this scenario into assumptions tied to physicality. To illustrate, let us apply RAT.

There are obvious ways in which the theory's applicability to cyber grooming and other forms of online abuse fall far short of the predictive and descriptive value it evidences for real-world crime. These mainly have to do with the fact that the theory was developed in an era in which online, anonymous, and technologically-enhanced offending were not possible. For example, definitions of what constitute adequate guardianship may have to be expanded to the point where the definition of the term loses its meaning and, therefore, its value as a variable of causality within the RAT model. Would an automated child protective software be considered guardianship? What about the physical presence of parents in the home; witnesses to publicly broadcasted abuse? Do

chat platforms differ from video-based ones in terms of which forms of guardianship may be helpful in different types of online abuse? How does one compare the relative value and impact of these and other potential forms of guardianship?

Though RAT treats both demographic characteristics and motivations as static predictors in its original "motivated offender" assumption, there is evidence that the demographic characteristics and motivations of online offenders vary significantly from those of traditional offenders (Hui et al. 2015; Marcum, 2007; Quayle et al. 2014).

In addition, the lack of specificity afforded definitions of *cyber presence* and *existence* undercuts the "suitable target" assumption by failing to define what "being present" in an online environment actually means. Would presence be defined as showing an online status using the social network's symbols; chat interaction with another user (without being present except as an observer of content); or simply having a personal profile in the "geographical locale," which in this case is a social network? Furthermore, would the temporal regularity of being present "only once" or more than once be measured by how many times the potential victim has indicated online activity (including a symbol, interaction activity, or posting activity), or would it mean regularity of using the social network in general (including intervals of logging into the platform)?

A further serious question is whether an online chat room or social network could be considered a crime scene. Yar (2005) argued that routine activities create opportunities for successful predation, that these activities always occur in a particular location and at a particular time, and that the application of RAT to cyber predation is, therefore, questionable because of the fluid spatio-temporal ontology of cyberspace compared to the physical world. Considering that RAT's "capable guardianship" is not strongly related to preventing risk-taking behavior among youth (Marcum et al., 2010), all three of the theory's propositions seem ill-suited to describing or predicting the etiology or accomplishment of online offending. As no structure and classifications exist for transferring RAT to the Cyber World, while accounting for the altered psychological and social variables in cyberspace, it appears to offer no accurate explanation and understanding of the phenomenon.

The criminological variables inherent in many of the theories applied to online offending are valuable in and of themselves, but as argued above, they lack the conceptual specificity required to make accurate predictions of behavior within the context of online environments. The imperative, therefore, should be to first evaluate a given theory for its appropriateness to describe a particular type of cybercriminal phenomenon and, then, determine whether it can be applied on its own merits, needs to be adapted, should it be rejected, or whether a new theoretical formulation specifically designed for cyber environments should be developed. It is likely that the behavioral variables in traditional theories that serve to explain the outcome of the phenomenon would not be as effective if the Internet was factored into the abuse process.

Similarly, as demographic characteristics commonly associated with offending in the physical world cannot be accounted for in the online world, psychological mechanisms that lead to sexual abuse or deviancy in the physical world cannot be expected to operate in the same way in the online world. In Ward and Seigert's (2002) pathways model of child sexual abuse as a psychological theory of sexual offending, four propositions were advanced in response to sexual offences: (1) intimacy and social skill deficits; (2) distorted sexual scripts; (3) emotional dysregulation; and (4) anti-social cognitions, each of which comprises a single pathway and distinct etiology. This theory was developed to explain child sexual abuse in the physical world, without taking into account the possible alteration of social and psychological variables brought by the Internet. Moreover, the theory did not consider the differences in the manner in which risk-taking and youth deviance would be expressed in the online world. In an investigation of the extent to which Ward and Siegert's model applies to online sexual offending, Middleton et al. (2007) found that almost half of their sample could not be related to the propositions of the model. In addition, Craven et al. (2006), in their review of the online grooming literature, considered Ward and Siegert's *pathways model*, together with three other psychological models on child sexual abuse developed for the physical world: Marshall and Barbaree's *integrated theory*, Hall and Hirschman's *quadripartite model*, and Finkelhor's *pre-condition model*. They argued that Ward and Siegert's pathways model concentrates more on the opportunity to offend, recognizing cyber grooming as actually creating an opportunity to offend. Moreover, they added that it would be inconclusive to integrate online child sexual abuse in these models, since the knowledge base on child sexual abuse 10 years ago would not apply to our understanding of child sexual abuse in the online world today.

Luring communication theory (Olson et al., 2007) captures the communicative process of entrapping the child in a sexual abuse setting, i.e., how the perpetrator lures the victim into this setting. The authors of the reviewed papers of the SLRA referenced this theory in the theoretical background of the grooming phenomenon. This theory has four propositions: (1) The luring process begins with gaining access to the victim; (2) the core of the phenomenon is the offender cultivating deceptive trust development; (3) deceptive trust development that leads to a cycle of entrapment as a process within (constituted by grooming, isolation and approach); and (4) communicative responses to sexual acts (the offender mitigating the response to the sexual act from the victim, e.g., persuading on the basis of secrecy).

While I would agree with their definition of grooming as "the subtle communication strategies that child sexual abusers use to prepare their potential victims to accept the sexual contact" (Olson et al., 2007, p. 241) and concur that deceptive trust development is a major characteristic of the grooming process, I also believe that this model has one core weakness. The data the authors used in building this model consisted of material on sexual abuse and pedophilia from the physical world, and online contextual environments were omitted. For example, by posing a "gaining access" proposition as the offender's active effort

toward beginning the cycle of entrapment, the model does not take into account the risk-taking and vulnerable behavior of the victim. Online victims often initiate the contact themselves (McGhee et al., 2011). In communicative theories of entrapment in physical settings, there is a gap in the explanation and prevention of the grooming phenomenon in terms of capturing the online context of the communication and its implications (McGhee et al., 2011).

2.3 Overreliance on static models of behavior

There is a heavy emphasis in CGOC research on identifying the motivations for engaging in grooming. This is an important issue (see, e.g., Birbeck & Lefree, 1993; Wikström, 2011), but most of this work is focused on identifying straightforward relationships between "static" personality characteristics and cyber grooming, resembling approaches more commonly found in clinical, behavioral, and personality psychology (see Allan et al., 2007; Hanson, 2009). The studies included in the SLRA primarily measured the relationship between individual differences and psychopathies—which are assumed to filter attitudes, beliefs, and perceptions in ways that motivate deviance—and cyber grooming. This dispositional orientation toward human behavior is referenced in an abovementioned work on the integration of cyber concepts into psychopathologies related to cyber grooming. Here, its role is more straightforward and, in the studies featured in the SLRA, seems to be focused on identifying those individuals in the population who are more likely than others to engage in CGOC.

The health psychology literature refers to these approaches as continuum models (Schwarzer, 2008; Weinstein et al., 1998) or non-stage theories (Velicer & Prochaska, 2008). Diagnosis of a disorder or condition is binary (e.g., one is either diagnosed as pedophilic or not) and thus "static." There is variation in terms of the degree to which the individual manifests the characteristics, symptoms, or diagnostics criteria associated with the diagnosis. Those who "score" higher on personality measures, or projective tests focused on a given trait or psychological profile, are subsequently assumed to be at greater risk of engaging in a related deviant behavior.

Forty-seven percent of the papers in the literature review focused on the motivation to engage in CGOC by referencing such dispositional models of human behavior that assume fixed rather than dynamic relationships between independent variables (e.g., personality constructs, individual differences, background characteristics) and cyber grooming (i.e., the dependent variable). The most common static explanations or predictors, modeled as independent variables, included the offender's characteristics, such as demographic (Aslan & Edelmann, 2014; Navarro & Jasinski, 2015), the psychological profiles of Internet offenders in general (Bates & Metcalf, 2007; Davidson & Gottschalk, 2011; Elliott et al., 2009), emotional avoidance (Wall et al., 2011), pedophilia (Durkin & Bryant, 1999; Holt et al., 2010; Howitt & Sheldon, 2007; Malesky & Ennis, 2004), cognitive

distortions (DeLong et al., 2010; Howitt & Sheldon, 2007; Hundersmarck, 2007; Whittle et al., 2013), and/or the psychological characteristics underpinning victim-related risk factors and vulnerabilities (Hof, 2011; Marcum et al., 2010; Mitchell et al., 2007; Wells & Mitchell, 2014; Whittle et al., 2013).

Identifying the profiles of offenders who are likely to engage in CGOC is worthy of study and may help in identifying at-risk populations for the purpose of prevention; there is also a body of work beyond CGOC that demonstrates this (see, e.g., Grann et al., 1999; Lösel, 1998; Roque et al., 2012). However, such static factors also have serious limitations. First, they are essentially organismic variables and, thus, are difficult to implicate in causal analysis (see Baron & Kenney, 1986; Lynd-Stevenson, 2007; Vale, 1969). Second, this means that these models cannot account for changes in the relationship between the variables and the cyber-grooming process. A simple example would be that online child abuse, modeled as the dependent variable, is caused by pedophilia, modeled as the independent variable. Such an explanation cannot account for situations in which the offender does not meet the criteria of pedophilia, as in the case of an offender who commits cyber grooming for the purpose of profit-orientated extortion (see Açar, 2016) or who is led to believe by the victim's virtual identity that he or she is not prepubescent. Additionally, explanations based on such continuum models do not support the opportunity to explore how independent factors and their relationships with cyber grooming might be changing dynamically via rapidly changing Internet interaction.

2.4 Inadequate process modelling

The final identified gap focuses on explanations employing stage or process models of CGOC, neither of which includes the victim's input within the process progression of the offender. Of the authors included in the literature review, 37% used process modelling. These studies either described how the act was committed in terms of steps (e.g., Barber & Bettez, 2014; Black et al., 2014; Hui et al., 2015; Kloess et al., 2014, 2015; Miah et al., 2014; Michalopoulos et al., 2014; O'Connell, 2003; Pranoto et al., 2015) or described the act using process models (e.g., Elliott, 2015; Kloess et al., 2014; McGhee et al., 2011; Quayle et al., 2014; Quayle & Taylor, 2003; Whittle et al., 2014).

While stage process modelling is very useful for exploring the nature of offenses that take place as discrete episodes (i.e., robbery, burglary, and other forms of one-on-one victimization), it is ill-suited for offenses such as CGOC, which take place over time and may involve multiple encounters and exchanges between offenders and victims. CGOC is similar to confidence- and deceit-based offenses, such as financial scamming or embezzlement, in that, it unfolds in a dynamic fashion according to the interplay between the offender (groomer) and the target (a child). Although the constituent behaviors and events transpiring during the offense are consistent, the exact progression of a grooming incident may vary significantly from offense to offense. Consequently, developing

predictive models or theories based on rigid processual typologies is likely to restrict the explanatory power of subsequent theories.

In addition, the usefulness of a stage model depends on how well the actual interactional paths of the victim and offender match the model stages. None of the models considered the influence of the victim's responses to grooming in varying the behavior of the offender. Even if offenders follow a consistent procedural script, it is difficult to imagine that they do not deviate from or adjust said scripts in response to how victims respond to them. Consequently, it is important to understand not only the individual behaviors of the offender and victim but also the interactional variables and to identify the risk and protective factors in CGOC.

The three most-cited models subscribing to this orientation are O'Connell's (2003) stage model of the steps an offender takes in online abuse, Quayle and Taylor's (2003) process model of problematic Internet use by people who have a sexual interest in children, and Quayle et al.'s (2014) process model of the ways in which an offender acquires the computer skills needed to offend.

Most stage models assume fixed relationships among their stages. For example, O'Connell's model (2003) suggests seven fixed steps that offenders take in perpetrating online abuse: (1) forming a friendship, (2) forming a relationship, (3) assessing risk, (4) exclusivity, (5) sexual abuse, (6) fantasy re-enactment, and (7) damage limitation. This is one of the first models to describe cyber grooming, and 45 of the 135 papers included in the literature review mentioned this model. For instance, Gupta et al. (2012) used this model to identify behavioral and linguistic patterns among pedophiles in chat conversations, and Black et al. (2014) used it in their linguistic analysis of grooming strategies. However, it has been proposed that offenders and victims tend to shift or skip stages (Elliott, 2015; Williams et al., 2013) or may use two stages simultaneously.[4] For example, in many instances, the offender does not progress gradually through bonding techniques toward online sexual abuse, as proposed by O'Connell, but might initiate a sexual conversation during the first few minutes of the conversation, expressing love and compliments later, usually after a few days of conversation. Common explanations for this are the anonymity, or at least the flexibility, of virtual identities and the Internet's lack of legal and social controls.

Likewise, Quayle and Taylor's (2003) process model on problematic Internet use fails to consider how the victim's input into the process might influence the offender's process. In addition, this model was created on the basis of data on offenders who downloaded child pornography, not those who performed cyber grooming. The skill-acquisition process model by Quayle et al. (2014) fails to consider the victim's input into the process, and its data sample

[4] Elliott (2015) suggested an integrated model based on O'Connell's model, in which he attempted to explain stage shifting by proposing a self-regulatory feedback loop in his offender's process model. This model does have limitations, the main one being that it focuses only on the process of gaining the compliance of another to achieve illicit goals, including cyber grooming, as a preparatory action. Elliott's model does not specify whether the mechanisms that it suggests for gaining compliance are exclusive to online communication, nor does it consider the victim's input.

was based on offenders' self-reporting. Although the interview questions were designed to assess the Internet's role, the model's stages did not introduce characteristics of the Internet as such. Instead, its stages simply abstracted the offenders' self-reported Internet behavior, and the model did not identify which of the Internet's roles triggers which of the model's stages.

3 A CONCEPTUAL MODEL FOR THE CYBER GROOMING OF CHILDREN

Based on the gaps and weaknesses deriving from the SLRA, existing work on CGOC is overreliant on traditional crime theories while failing to account for the unique effects of the Internet as a causal factor connecting offender motivation and victim vulnerability in cyber grooming. Moreover, there is an overemphasis on static dispositional factors and process-oriented factors in predicting CGOC. In the next section, I present the conceptual model appraisal as a response to the major shortcomings identified in the extant literature on cyber grooming.

3.1 Responding to the lack of cyber specificity

To address this gap, future research should incorporate and measure cyber-specific variables that implicate separate online-specific behaviors within the cyber-grooming process. In the context of cyber grooming, research has thus far viewed the Internet as a tool or platform for the perpetration of abuse that is no different from that encountered in the physical world. GA suggests that we should acknowledge and measure how cyber- or online-specific factors uniquely influence offending (in most cases, as a mediator or moderator of the relationship between motivation, opportunity, and offending). For example, cyber-enabled anonymity may trigger someone who would not have committed a crime in the physical world to do so online. Further, the lack of legal enforcement and social control on the Internet make it easier to commit crimes there than in the physical world. At the same time, we do not know the specific manner in which Internet contexts affect grooming strategies and offending behaviors or how they condition the vulnerability of victims. For example, anonymity can be achieved in a variety of ways (e.g., false identities, multiple profiles, voice or image distortion technologies, use of incognito tabs in communication or browser software, etc.). Each of these techniques may have unique effects on potential victims based on their age, gender, experience with the Internet, or situational

emotional status, beyond the collective observation, with the Internet being used as a tool to perform CGOC.

I propose incorporating and measuring cyber-specific variables that implicate separate online-specific behaviors in the cyber-grooming process based on online disinhibition. The literature conceptualizes Internet behavioral dissonance as online disinhibition, the primary conceptualizations of which acknowledge positive and negative, or benign and toxic, online disinhibition (Joinson, 2007; Suler, 2004). Suler (2004) introduced the internet disinhibition effect, which states that six Internet attributes enable users to behave differently in the online world and may even trigger the "hidden offender." Jaishankar (2008), who also argued that people behave differently in different spaces, proposed space transition theory, in which "Identity flexibility, dissociative anonymity, and lack of deterrence in cyberspace provide offenders choice to commit cybercrime" (p. 2). In addition, regarding online sexual offenses, Coopers (1998) characterized the Internet as a "triple A engine" (anonymity, affordability, accessibility) that drives online sexuality. These early conceptualizations set the standard for what is thought to trigger alterations in online behavior, yet none of them specified the relationship between their constructs and outcomes, in this case, cyber grooming. We do not know how the offender and victim use each of these Internet attributes in the grooming process. This arguably prevents us from providing an explanation of how these Internet characteristics can actually indicate criminal behavior, something that could potentially provide great insight into preventing this type of crime.

3.2 Responding to the overreliance on traditional theoretical formulations

Second, incorporating such cyber affordances as, perhaps, primary causal factors within the phenomenon of analysis could help in addressing the theoretical gaps in the literature analysis, specifically in terms of the overreliance on traditional theory. I maintain that cyber phenomena require new conceptualizations to accommodate the unique nature of online environments. For this purpose, cyber-specific variables ought to be situated within the cyber-grooming process as a form of conceptual specificity that is required to make predictions of behavior within the context of online environments. Such an approach does not abandon the traditional approaches to crime prevention, the study of cybercriminal and deviant behavior, or the psychological background of the phenomenon of interest. On the contrary, it creates a new instrument for studying the phenomenon, equipped to sustain the "foreign air pressure" (i.e., the cyber environment) and adds a "three-dimensional" view in explorations of known phenomena (adding the cyber dimension within the existing theoretical and modelling concepts of sexual predation of children). Research can then dissect any other existing or future cyber phenomenon in their natural environment.

3.3 Responding to the overreliance on static models and inadequate process modelling

Third, to address the CGOC-related modelling gaps, I suggest the measurement of cyber-specific variables, as they are interactively used by both the offender and victim during the cyber-grooming process. Such an exploration will offer potential for a dynamic spatio-temporal organization, as well as solutions to mapping a phenomenon characterized by interactive components, and will help overcome issues of static-dispositional and fixed-relationship situational factors. The reasoning is that we could fit the explanation of how a car works into a stage model, but the spatio-temporal organization of that stage model would not identify the interaction among all the working parts that produce stage-level observations. Exploring and mapping the use of cyber affordances during the offender's and victim's paths in the grooming process (expressed in the theme of abuse as the resultant behavior) shall provide valuable and much more detailed insight into the phenomenon.

3.4 A cyber affordance model of cyber grooming

The concept of affordances was first introduced by Gibson (1977) as information available in the environment, seen or unseen, that communicates different possibilities of action. The concept has been receiving attention from IS scholars in exploring technology as an enabler of different behaviors (Bernhard, Recker, & Burton-Jones, 2013; Leonardi, 2013; Majchrzak & Markus, 2012; Markus & Silver, 2008; Pozzi, Pigni, & Vitari, 2014; Seidel et al., 2013; Volkoff & Strong, 2013; Yoo et al., 2012; Zammuto et al., 2007). Thus, within the IS discipline, this concept is used primarily for explaining the use of IT in organizations and organizational change (Pozzi et al., 2014).

In an attempt to open up the black box and show the inner workings of an internal phenomenon (Hedström & Ylikoski, 2010), I conceptualize cyber-exclusive variables as "cyber affordances" that pose as variables measuring the interaction between the offender and victim (Figure 2).

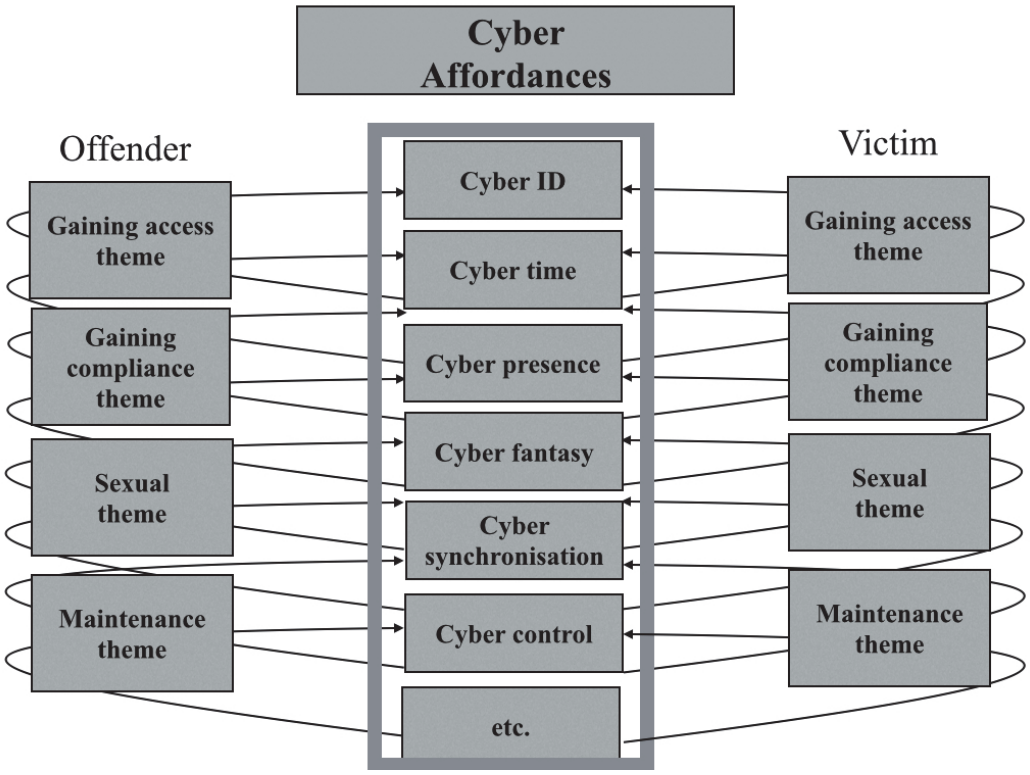


Figure 2: Cyber affordance model of cyber grooming

Table 1: Cyber Affordances as Conceptual Variables

Cyber affordance	**Conceptual variable description**
Cyber identity	Expressing and discussing identity-related parameters, such as name, age, gender, and location
Cyber presence	Online manifestation of identity-related parameters, such as photo, video, voice
Cyber time	Online status and asynchronized online presence
Cyber fantasy	Abstract image construction (imaginative state) achieved through online text exchange
Cyber synchronization	Towards achieving stability and assessing the potential of practicing imaginative states (leveling of the minds of the actors in the communication)
Cyber control	Evaluating the risks of the established relationship or exchanged communication in regard to law enforcement or social control, risk awareness, and trust control

Cyber affordances are based on Suler's (2004) online disinhibition affect. Suler (2004) advanced the six Internet attributes with a high level of abstraction and as a philosophical argument. Raising these attributes to the level of conceptual variables to be measured in chats is an attempt at discovering behavioral linkages between the silent possibilities of actions that cyber environments may communicate to their users in the case of CGOC (Table 1). I now discuss these cyber affordances in detail.

Cyber identity refers to how actors in an interactive chat would express actions fomented by the anonymity allowed in cyberspace. This is not to assess whether or not the actors are misrepresenting or untruthful. The actors in many online communications, including cyber grooming, cannot be sure of the veracity of the identifying parameters provided because online communication facilitates deception. This conceptual variable identifies the way in which actors might misrepresent themselves by using various identifying parameters in interactions with others.

Cyber presence refers to the premise of most people that, online, we are invisible. In the physical world, one could not walk into a room with three people without making our presence at least noticed. Online, one could be browsing Facebook without the knowledge of others, or one could follow a group-chat interaction without the chat-group participants' awareness. Users are allowed to do this by simply choosing not to reply to a message, manually modifying the social network symbol to "hide," or not providing information regarding availability. In the physical world, people would also notice what you wear, how you wear your hair, or even your mood or intentions by only being present in a certain locale. Online, you build this presence by uploading photos, videos, creating Instagram feeds, subscribing to interest groups, and so on. This cyber presence, as conceptualized in this work, is a variable that would capture the way in which chat participants form their presence.

Cyber time refers to the possibility of asynchronous communication in the chat. It concerns whether actors manifest or respond to time-binding matters within the chat and in which form. In the physical world, or in face-to-face communication, it is difficult to mask one's availability, or delay a response, due to the physical proximity of the communicator. Online users, however, can purposely delay a response to a message or even manipulate the time frame within which they respond. Today, we can schedule the sending of emails or even manipulate when we have "seen" the message through the "seen" time stamp. Thus, users appear to be able to create their own time dimension, detached from the physical world. This variable can manifest itself within online chat communication by assessing or acquiring information regarding the next time a designated actor would be online. It may also present itself as whether the actors identify their unavailability (e.g., "I am away from keyboard") or whether they react to a significant time delay between responses, and in which form. Future research may even employ the "seen" time stamp to assess certain behavioral outcomes.

Cyber fantasy builds on dissociative imagination. It captures the notion of self-detachment from the physical world, as expressed by the actors in an online exchange. Online, people can feel uninhibited about expressing fantasies that they would not normally express, especially in the physical world. This can be done by identifying abstract imaginative states within the messages exchanged in the chat. For example, actors describing their everyday lives, their physical or personal characteristics, or perhaps making up scenarios of what could happen in the future can all be considered imaginative states. Again, it is not the variable mandate to capture whether these abstract images are true or false or whether they are grounded in the actual physical life of the actor expressing them. Such information can also be easily misrepresented and extremely difficult to assess when studying online communication. However, cyber fantasy captures how the actors take the "liberty" to practice the textual expression of imaginative states, which could also open up the possibility to further explore whether such imaginative states affect subsequent behaviors.

Cyber synchronization embodies solipsistic introjection or the merging of minds between two users in online communication. In the physical world, or in face-to-face communication, it is much more viable to assess whether a message communicated in real time has a positive, negative, or perhaps ironic or threating tone. We can achieve this by interpreting facial expressions, social cues, body language, etc., which inform our judgment of how to react. Online, many messages are not accompanied by such cues. We often find ourselves doubting or re-reading an email, trying to determine or even imagine the tone of what the sender has said. Suler (2004) described this as "a voice within one's head, as if that person's psychological presence and influence have been assimilated or interjected into one's psyche" (p. 323). If the doubt persists, we then, perhaps, either ask for clarification for a certain aspect of the email text or, alternately, hope for the best or dread finding out the contrary until we have met the email sender in the real world. Although it would be almost impossible to empirically assess whether an actor in an online chat communication projected a voice of their communicative party in their head, it does not mean that this attribute should be dismissed. The impulse to request clarification of a tone or the meaning of a message can be interpreted as levelling or synchronizing the mind between the communicative parties during the chat communication. In malicious chats, such as cyber grooming, the tone, or these synchronizing behaviors, can also be manipulated toward abusive goals. In turn, this variable could be manifested in behaviors in the chat, such as asking for additional confirmation, or clarification, maybe persuasion (as in "twisting the hand" of the actor), manipulation, or even aggression in the responses. Future research might also perform sentiment analyses in order to refine cyber synchronization or even study the use of emojis in this affordance.

Lastly, *cyber control* relates to the minimized status and authority that online users may experience as a product of lack of centralized formal or informal social control over the internet (e.g., a by-stander on the street or a police car passing by). This conceptual variable would seek to determine behaviors in the chat that

would potentially prove minimized authority or control. One might argue that the whole cyber-grooming chat can be proof of such minimized authority, since grooming should be considered illegal and deviant. However, an offender might omit to think of his contact with the victim as illegal due to somehow believing that the victim is over 18 or, even more so, not considering the grooming act as wrong, perhaps due to cognitive distortions. Thus, thinking of minimized authority in such a broad sense would perhaps exclude the richness of this attribute, which might be evident in the actual chat communication. Therefore, this variable would assess minimized authority as "crumbs of bread" within the chats regarding whether the actors express notions of minimized authority and control in relation to what they are discussing. This could range from discussing whether they are alone in the room while chatting to expressing acknowledgment that what they are doing is wrong and being reported to the police. I believe that the expression of these notions would be an adequate representation of the possibility of having "no control" over the Internet.

For the purpose of the model in Figure 2, in order to characterize the offender–victim interaction, I used an integrated knowledge of several cyber-grooming process models (Barber & Bettez, 2014; Elliott, 2015; Craven et al., 2006; O'Connell, 2003; Olson et al., 2007; Quayle et al., 2012; Webster et al., 2012; Whittle et al., 2013; Williams et al., 2013) and define the themes as: (1) gaining access, (2) gaining compliance, (3) sexual abuse, and (4) maintenance (Table 2).

This dissertation treats these themes as the resultant behavior of cyber grooming because it assumes that the abuse process begins with the first and ends with the last message in a cyber-grooming chat log and that each message could be categorized into a certain theme according to its content and context. Each theme composing the cyber-grooming process was formed by an abusive or potentially abusive interaction. Thus, online communication is a two-way street. The offender's input messages influence the victim's input messages, and the offender may demonstrate one theme, while the victim demonstrates another in response. To accommodate this, I identify two parallel, duplicate processes, one for the offender and the other for the victim, and I suggest that the offender and victim travel through their own separate grooming process themes while using the cyber affordances (Figure 2). Future testing of the proposed model structure against data on cyber grooming might reveal relationships regarding how the cyber affordances are used during cyber-grooming behavior.

Table 2 Offender/Victim Themes and Subthemes in the Cyber-grooming Process – Integrated

Offender/Victim Themes	Offender/Victim Subthemes	Description
Theme 1 Gaining Access	Initiating contact	Introductory messages
	Assessment	Assessing the individual characteristics of the offender; the individual characteristics of the victim/offender regarding potentiality, while getting to know each other; assessing the environment (location, family, and relationships), willingness, and availability; sexuality assessment, assessment of sexual experiences
Theme 2 Gaining compliance	Building rapport	Simulating friendship/romance, coordination, predictability, and stability of behaviors; mutuality—mutual attentiveness and interests; positivity—friendliness, empathy, and warmth, manipulation, overt manipulation, liberal thinking, mirroring
Theme 3 Sexual abuse	Sexting	Exchange of text messages with sexually explicit or sexually implicit content and/or context
	Producing, distributing, possessing CAM	Requests for/or creation, exchange and distribution of child abusive material (CAM) (exchange of images, video)
	Streaming	Requests for/or webcam streaming as part of the sexual context
	Physical Abuse Potential	Assessing the potential and possibility for a meeting in the physical world, discussing previous meetings in the physical world
Theme 4 Maintenance	Assessing risk	Assessing the likelihood of activities being detected by, for example, the child's parent(s), guardian, older siblings, or law enforcement.
	Control and Harassment	Bribery, gifts, money, force and threats, integrity projection, suffering, insidious controlling, intimidation and fear, blackmail

4 EMPIRICAL STUDY

This dissertation is an empirical study and treats the above-presented conceptual model as a prescription for research. It aims to dissect the cyber-grooming phenomenon in its natural environment by using chat-log transcripts of real-life cases of cyber grooming. Its first aim is a qualitative exploration of whether, and the extent to which, the offender and victim manifest use of conceptual cyber affordances during the cyber-grooming process. Thus, the primary empirical mandate of the study is to use cyber-grooming themes to explore the specific cyber affordances being used as well as how both the actors in the chat, the victim and offender, use these affordances vis-à-vis the themes emerging from the cyber-grooming process. The study also uses chat-log time stamps to provide a descriptive insight, through a spatio-temporal lens, into how cyber grooming is committed. Ultimately, it aims to illustrate future research potential and provide recommendations for the future prevention of online child sexual abuse. Consequently, it answers the following research questions:

RQ1: What form do the chat-based cyber affordances take?
RQ2: How do the offender and victim utilize the cyber-grooming themes as the chat progresses?
RQ3: Which of the cyber affordances are most frequently deployed in the chats?
RQ4: To what extent are cyber synchronization, cyber fantasy, and cyber control being used under the sexting, CAM, and physical abuse potential themes?
RQ5: What information can the cyber affordances and themes provide for evaluating the urgency of physical abuse potential according to the time stamp?

4.1 Research approach

To understand the use of cyber affordances, I adopt an interpretive research approach using qualitative hermeneutic content analysis in combination with quantitative analysis on tabulated qualitative codes. As the literature analysis has shown, there is an abundance of information on how specific Internet behavioral characteristics are used during the cyber-grooming process. An interpretive approach is desirable when a phenomenon possesses high social and contextual complexity (Bhattacherjee, 2012), particularly social phenomena that are composed of interactive human action, which are both context- and time-dependent (Orlikowski & Baroudi, 1991). I believe that cyber grooming is a vivid example of such a phenomenon, where actors communicate and demonstrate novel behavioral patterns through the Internet and chat-interactive platforms. As such, in my empirical study, I shall engage in a "sense-making" process of discovering these Internet-specific behavioral characteristics and how they interact with the behavior of actors during the cyber-grooming process. Such "sense-making" aims to build theoretical foundations for future research as well as practical recommendations for cyber-grooming and cybercrime practitioners.

4.2 Interpretative research

Interpretative research in information systems behavior is a well-established research approach, with leading journals publishing interpretive studies aimed at understanding IS behavior (Cecez-Kecmanovic et al., 2014; Sarker, Xiao, & Beaulieu, 2013; Walsham, 1995, 2006; Yoo, 2010). The interpretive perspective attempts "(…) to understand the intersubjective meanings embedded in social life … [and] to explain why people act the way they do" (Gibbons, 1987, p. 3, taken from Orlikowski & Baroudi, 1991).

Similar to Orlikowski (1989), I state my theoretical framework upfront in the form of a conceptual research model that provides information about the use of internet-specific characteristics, i.e., affordances, in order for the reader to understand the biases or blinders I might bring to the study. The pre-conceptualization of the major categories, composed of "cyber affordances" and "themes," outlined in the previous section of my thesis will be used as an enactment of the social reality that I am studying. With this, I adopt a strong constructionist approach, as I believe that "there is no direct access to reality unmediated by language and preconceptions" (Orlikowski & Baroudi, 1991, p. 15). In this sense, my exploration is, in fact, how this pre-conceptualization (the cyber affordances and cyber-grooming themes) can be manifested through actual behavior within the cyber-grooming process. Therefore, the positioning of the conceptual model and cyber affordances is not an a priori theory to be tested, yet a construct of disciplined imagination shall guide the interpretation of the findings from the empirical study (see Walsham, 1995).

4.3 Methodology

In this study, I used a combined-methods approach, the use of which is now encouraged in IS research (see Venkatesh, Brown, & Bala, 2013; Zachariadis, Scott, & Barrett, 2010). As interpretative research relies heavily on qualitative research data, combining the qualitative approach with quantitative methods can generate unique insights into complex social phenomena (Bhattacherjee, 2012). Since chat-log data of real-life cases of cyber grooming are time stamped and unique, I have decided to dive into an exercise of discovering the potential of quantifying the qualitative codes deriving from the content analysis in order increase the richness of the qualitative data and the possible practical recommendations from the findings.

As part of the qualitative analysis, I first employed a hermeneutic content analysis (Bhattacherjee, 2012; Elo & Kyngäs, 2008) to discover the manner in which the pre-conceptualized cyber affordances and themes are manifested during the cyber-grooming process. From the qualitative codes arising from the content analysis, I then employed quantitative techniques by constructing panel data (time-series cross-sectional data) from the codes based on their unique time stamp in the chat log (Wang, Meister, & Gray, 2013; Duan, Gu, & Whinston, 2008; Hitt, 1999). I then employed a descriptive analysis using STATA.

4.4 Data collection

Previous research on cyber grooming is heavily reliant on data gathered from incarcerated offenders or probationers in treatment (Durkin & Bryant, 1999; see also Babchishin et al., 2015; DeLong, Durkin, & Hundersmarck, 2010; Howitt & Sheldon, 2007; Laulik, Allam, & Sheridan, 2007; Navarro & Jainski, 2015) or youth who are at risk of cyber grooming (see Mitchell et al., 2004; Mitchell, Finkelhor, & Wolak, 2007; Nielsen, Paasonen, & Spisak, 2015; Wasch, Wolf, & Pan, 2012). This is perhaps due to the fact that gaining access to the digital interactions from this cyber phenomenon is extremely difficult, primarily because of its criminal nature.

Very rarely does the study of cyber grooming unearth data in the form of chat logs of real-life abuse cases (see Eneman et al., 2010; Kloess et al., 2015; Quayle et al., 2012). Researchers need to face legal and ethical considerations due to data sensitivity and the confidentiality of the actors involved (one of whom is always a minor). Most of the research deploying chat logs as digital interaction data in cyber grooming has used chat logs from the website Perverted Justice. This platform allows public access to chat logs of cyber grooming in which the victim is an undercover volunteer pretending to be a child in order to attract predators for future convictions (see Albert & Salam, 2012; Black et al., 2014; Gupta et al., 2012; McGhee et al., 2011; Williams, Elliott, & Beech, 2013). Limitations of research utilizing such data raise questions such as the extent to

which the "agent provocateur" behavior of the volunteer affects the behavior of the offender or the extent to which the natural state of the phenomenon and its explanations are altered or impaired, given that the volunteer is an adult and not a representative of the actual vulnerable group.

In interpretative research, social phenomena should be studied in their natural setting (Bhattacherjee, 2012). "This implies that contextual variables should be observed and considered in seeking explanations of a phenomenon of interest, even though context sensitivity may limit the generalizability of inferences" (Bhattacherjee, 2012, p. 106). In light of this principle, I aimed for data in a form of chat-log transcripts of real-life cases of cyber grooming, since they represent a record of the phenomenon occurring in its natural setting.

The data was obtained through the Finnish NBI between the spring of 2016 and the autumn of 2019, following security clearance for myself and both of my supervisors (Tutkimuslupa ID-1716908).

4.5 Data set

For the purpose of this dissertation, the empirical study depicts a data set containing fourteen cyber-grooming chat logs between one convicted offender and his fourteen victims, who were abused between 2013 and 2014. Each chat log represents the unique chat-interactive communication between this offender and one victim, respectively. The data analysis was performed in the IT faculty, University of Jyväskylä, following a security protocol arranged by the Finnish NBI and the IT faculty. For the data analysis, the chat-log data were first anonymized and then translated from Finnish to English with the help of a fellow researcher from the IT faculty, who was approved by the Finnish NBI.

The offender was Finnish male, a single, unemployed Caucasian in his late 30s during the abuse period, with no higher education. The mean age of the victims was 13.7 years in the abuse period, all of them female, Caucasian, and Finnish. The offender met the victims over a popular social media platform in Finland, where he procured their Skype address through the personal details section published on their social media platform profile.[5]

The chat communication in the chat-log transcripts between the offender and his victims was achieved over Skype. The mean days of active conversation between the offender and the victims was 22.9 days. This means that the offender and victims were in contact between 2013 and 2014 and actively chatted for almost 23 days between the beginning and end of the contact. The mean chat-log length was 1,052 lines, and the chat-log transcripts comprised 12,950 lines in total.

[5] Additional information on the case in terms of offender apprehension, prosecution, and sentencing was omitted in consultation with the Finnish NBI due to confidentiality and preservation of anonymity.

4.6 Data analysis and model operationalization

In the previous section, I presented the cyber affordance model of cyber grooming as a novel theoretical model that embodies the cyber contextualization of the phenomenon. I also suggested an exploration of cyber affordances as conceptual variables that might facilitate cyber-grooming behavior in the online environment. Here, I provide an illustration of how the conceptual model (Figure 2) is used as a construct of disciplined imagination, which will guide the interpretation of the findings from the empirical study (see Walsham, 1995).

A content analysis of each message assigns the message to themes relating to abuse, and a parallel analysis of the same message identifies and reveals which cyber affordances are being used in the chat. For example, introductory messages belong to the gaining access theme, and messages containing sexual content and context belong to the sexual abuse theme. At the same time, a message that mentions identity-related parameters belongs to the cyber ID theme; one that mentions imaginative states belongs to cyber fantasy; and one that mentions disclosure to parents belongs to cyber control.

The temporal aspect of the chat log will then enable us to follow the dynamics of the process. In chat logs, each input, whether from the offender or victim, has its own time stamp, signifying the exact time it was sent as the chat progressed linearly through time. This means that by following the progression of the time stamp after the assigned cyber characteristic and theme through the content analysis of each message, we can observe the circulation of the use of the cyber affordances throughout the grooming process. Let us take the following adapted example of a grooming chat-log extract:

A. Offender says: 21:17:29: My name is Nemo, 17-year-old guy from Helsinki
B. Victim says: 21:20:50: Do you have a girlfriend?
C. Offender says: 21:30:00: You could be my girlfriend if you send me a naked pic!

If we apply content analysis to the offender's interaction in A above, ("21:17:29: My name is Nemo, 17-year-old guy from Helsinki"), we can place that message in the offender's gaining access theme, as the offender is using a cyber ID, including a name, age, gender, and location as the properties of that cyber ID. The same process can be used for the victim's responses by entering the time stamps of the victim's input responses (B) according to their themes and use of cyber affordances. For example, when the victim replies to the offender's message with B = "21:20:50: Do you have a girlfriend?" we categorize this reply in the gaining compliance theme. A content analysis of this message identifies that the victim is using cyber synchronization by seeking approval from the cyber affordances (Figure 3).

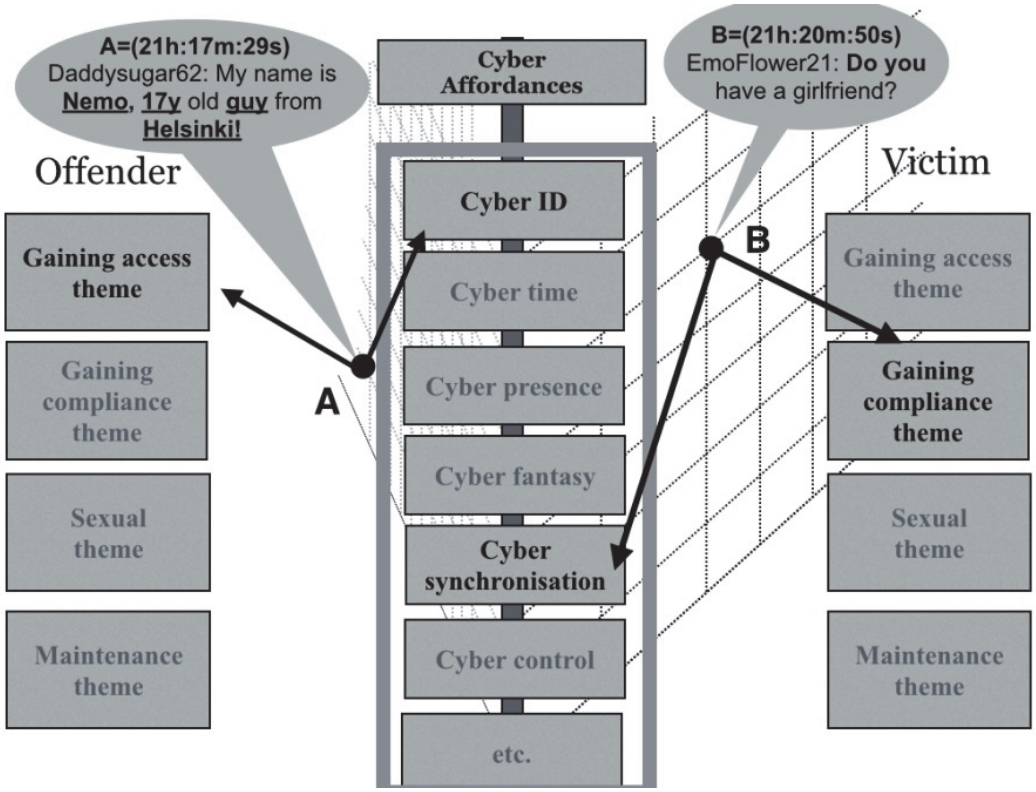


Figure 3: Model operationalization (example 1)

Next, when the offender replies to this victim's message with C:"21:30:00: You could be my girlfriend if you send me a naked pic!" the time stamp marks C = sexual abuse theme, and C = cyber synchronization and cyber fantasy affordances (Figure 4).

By following the time stamp progression of the interaction in the example from Figures 3 and 4, we can identify that the use of the cyber ID by the offender has triggered the use of cyber synchronization by the victim (A→B in Figure 5). We can then see that the use of cyber synchronization by the victim (B) has triggered the use of cyber fantasy and enhanced cyber synchronization in the offender (B→C in Figure 5). With this analysis, we would also be able to further explore which cyber characteristic appears most frequently and which is most active during the most aggressive themes of the abuse—both of which could help improve prevention awareness and Internet security policies.

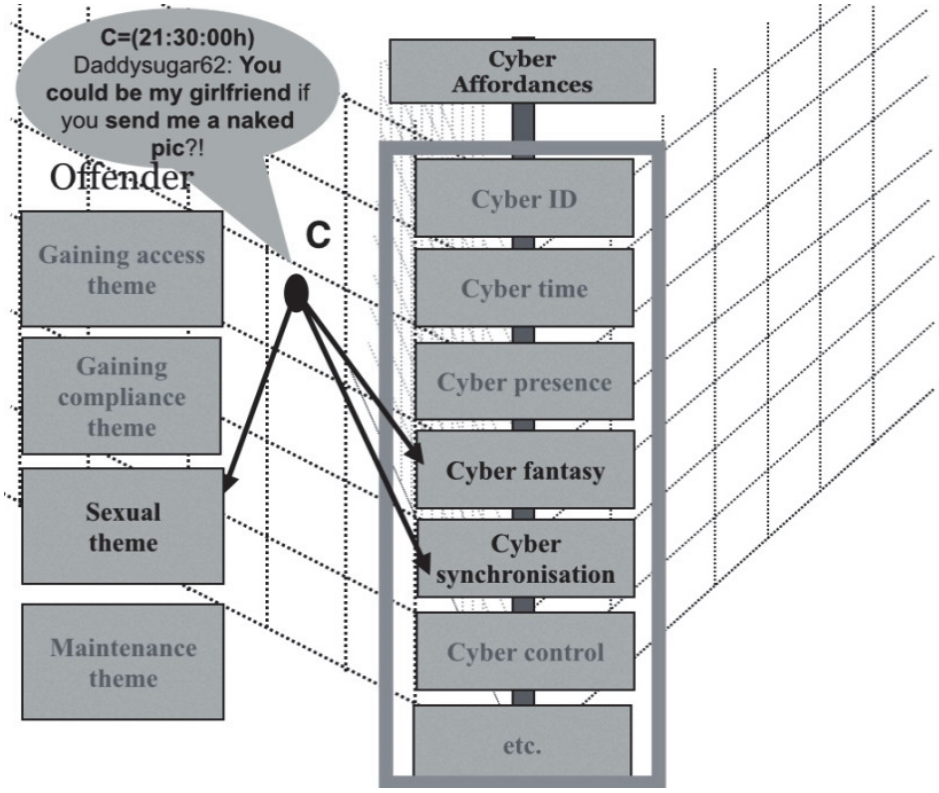


Figure 4: Model operationalization (example 2)

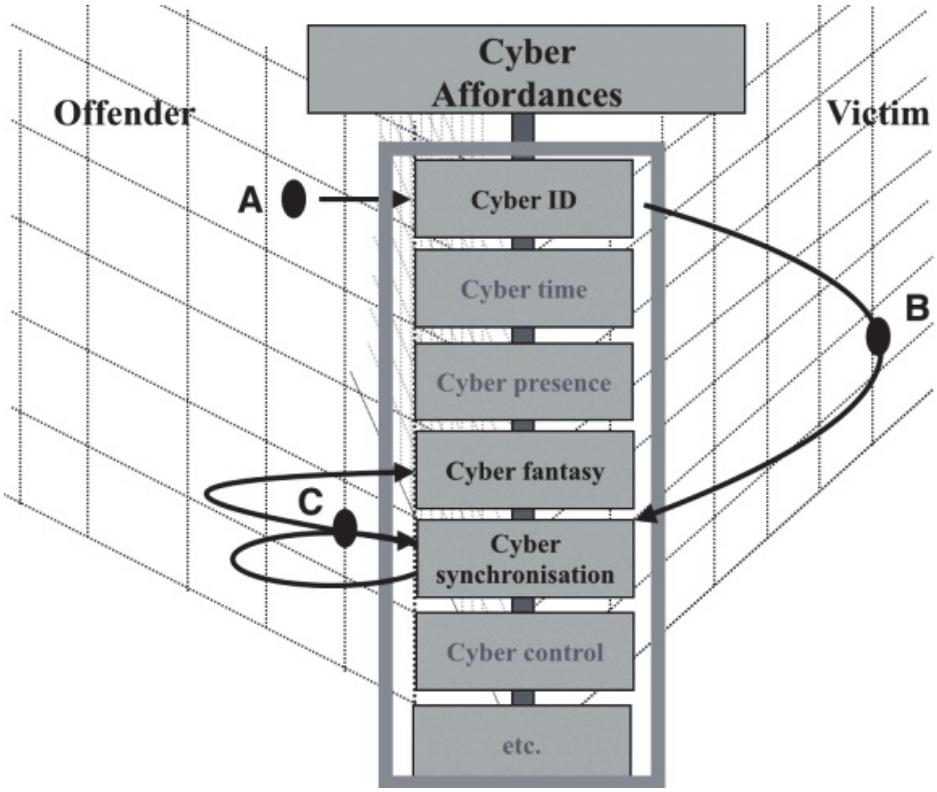


Figure 5: Model operationalization (example 3)

We can also identify which of the offender-related themes triggered which of the victim-related themes, and vice versa, and due to the time stamp of each theme activation, it might be possible to determine the average time between each theme activity. From the example in Figures 3 and 4, we can see that the offender has initiated the conversation with the gaining access theme, while the victim has replied with a message characterized by gaining compliance, which has triggered the offender's sexual theme message (A→B→C Figure 6). These future explorations can provide insights into the timing of law-enforcement intervention. With such insight, we can strive toward cyber-exclusive situational crime prevention.

Furthermore, we could explore the developmental path of the offender or victim, using this process for either actor, in relation to the themes as well as the use of the cyber affordances in correlation with the themes (Figure 7). For the example in Figures 3 and 4, we can identify that the offender jumps from the introductory message in the gaining access theme to the sexual theme ((A→C≠B in Figure 7). With such explorations in the future, we would be able to develop cyber-exclusive criminal scripts aimed at cyber offender and victim profiling or even cyber offender registers in aiding law enforcement investigations and child welfare.

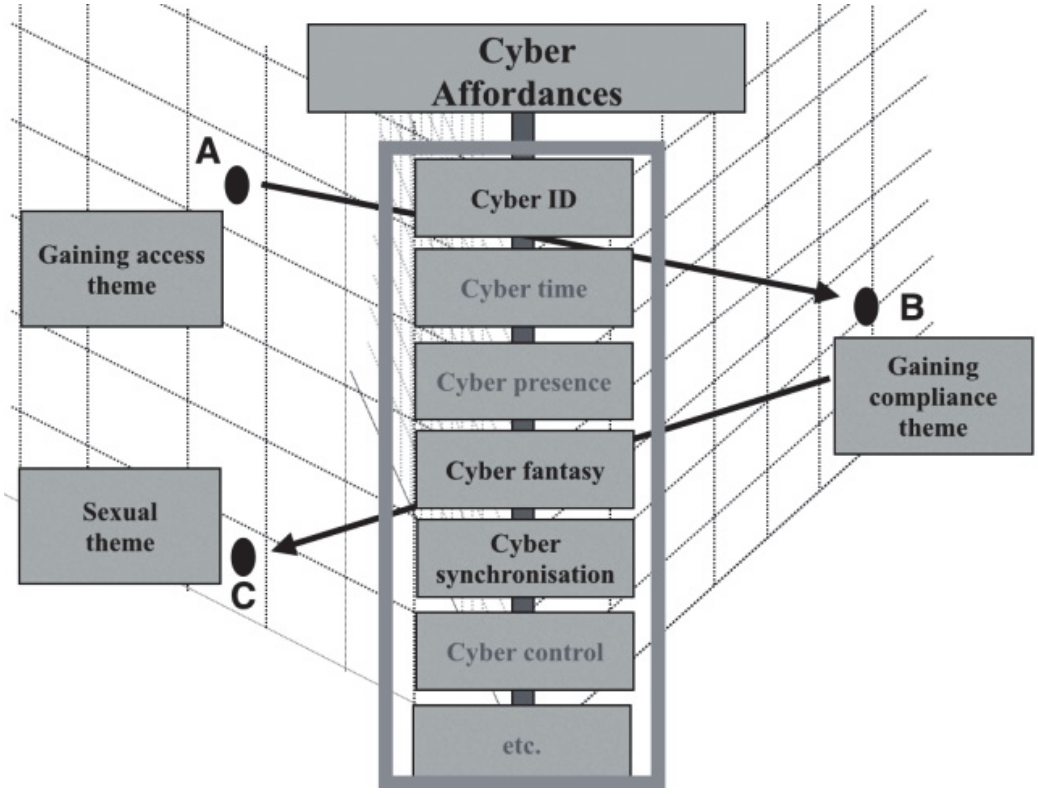


Figure 6: Model operationalization (example 4)

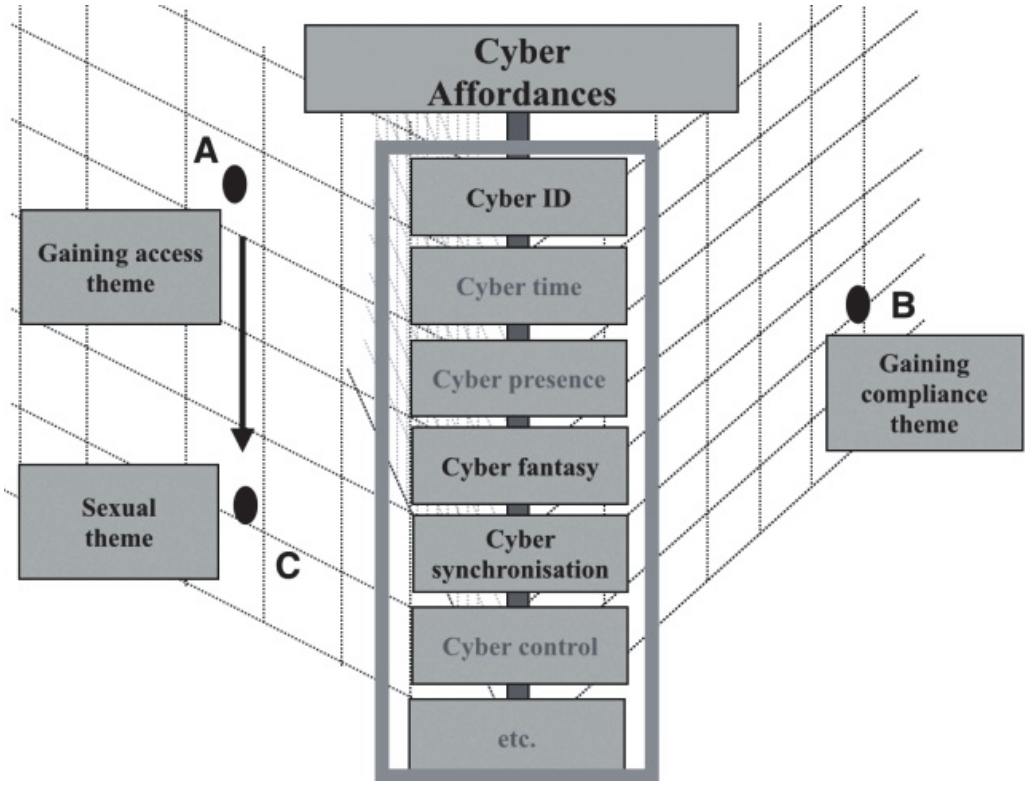


Figure 7: Model operationalization (example 5)

4.7 The qualitative analysis

Content analysis is a research endeavor in which the researcher is used as an instrument to interpret the subjective meaning of written, verbal, or visual communication messages (Bhattacherjee, 2012; Cole 1988; Elo & Kyngäs, 2008). It consists of the researcher applying one or more concepts to text segments through a coding process, which is calibrated by the explanations that the researcher wishes to uncover (Bhattacherjee, 2012). The coded data can then be analyzed, often both quantitatively and qualitatively, in order "…to determine which themes occur most frequently, in what contexts, and how they are related to each other" (p. 116).

4.7.1 Coding procedure

The content analysis in this study employed two coding matrixes: a structured matrix and an unconstrained matrix (see Elo & Kyngäs, 2008). The structured matrix consisted of a priori categories (see Appendix 2) depicting the themes in the grooming process for both the offender and victim, as they occurred in the chat. Each message from the chat transcripts was assigned a single code, and only aspects that fit the matrix of analysis were chosen from the data. This matrix

helped determine the spatiality of the offender's and victim's behavior, respectively, within the cyber-grooming process. Let us take another adapted example. By following the structured matrix from Appendix 2, we have input and output messages time sequenced and naturally occurring in this manner:

A) Offender says*: Hello!*
B) Victim says: *Hello!*
C) Victim says: *How are you?*
D) Offender says: *I am always good when I think of your p*ssy!*

Message (A) is coded with OT1 (offender introductory messages), message (B) is coded VT1 (victim introductory messages); message (C) is coded VT3 (victim rapport building); message (D) is coded OT5 (offender sexting).

Following the principles of inductive content analysis, however, the unconstrained matrix reveals the different categories (the sub-affordances) used under the general category of a specific cyber affordance. Within the unconstrained matrix, each message exchanged in the chat can contain multiple codes. This is due to the fact that one message can represent multiple contexts or no context at all if the message is a follow up. For example, following the unconstrained matrix from Appendix 3, we have input and output messages that are time sequenced and naturally occurring in this manner:

E) Offender says: *I am thinking of f*cking you hard!*
F) Victim says: *Well I am not!*
G) Offender says: *Why?*

Message (E) is coded with x4(1), depicting explicit fantasy, while messages (F) and (G) read independently from message (E), as it is void of explicit fantasy content, though not explicit fantasy context. Therefore, first, the x4(1) code assigned to the offender's message (E) is copied to the victims message (F), and an additional code, dismissal x5(4), is added to victim's message (F), depicting the victim's dismissal of the offender's explicit fantasy. We know that the dismissal relates to the explicit cyber fantasy. Next, the offender's message (G) is coded with x4(1), x5(4), and is assigned a new code x5(1), seeking approval. Thus, we know that the offender's seeking approval relates to the victim's dismissal of explicit fantasy. Messages with multiple contexts were coded with the same logic, with each message then carrying a string of codes in regard to a separate contextual belonging. With such coding, I sought to maximize the data contextual richness, which could be lost due to the nature of chat-log data when only single codes were used per message.

4.8 The quantitative analysis

A quantitative analysis was used as an explanatory boost for the qualitative codes. It was not used as a generalizable statistical report of the sampled population. It was simply a means to better present the qualitative data from the sampled population and to increase the explanatory power. This approach also strove to present the potential of such insights for measuring the occurrence of the behavior, as represented in the qualitative codes for the purpose of behavioral profiling, and intervals of the occurring behavior for the purpose of timely law enforcement prevention.

The qualitative content analysis was then used to construct panel data (time-series cross-sectional data) (Duan et al., 2008; Hitt, 1999; Wang et al., 2013). The panel data were constructed by first using the COUNTIF command in Excel to identify and tabulate the qualitative codes as dummy variables. The time stamps of each line in the corresponding dummy variable were then set as a time variable. Empty observations were added for each chat to reach the maximum line length of the longest chat (3,600 lines). In total, the data set contained 12,950 unique data points. The data were then transferred to STATA.

In addition to the descriptive analysis presented in the findings section, I present the results of performing a regression analysis on the occurring qualitative codes in Appendix 4. These results were omitted from the main text of this dissertation due to the limited generalizability of the logistic regressions and the small sample size of only 1 offender and 14 victims, who varied among the data sample. However, they were included as auxiliary material, since the data set comprised 12,950 data entries or chat lines with their assigned qualitative codes in STATA. The aim was to demonstrate proof of the concept and the potential of studying chat logs in this manner in the future, with improved and more versatile data sets.

5 FINDINGS

5.1 Identifying the cyber affordances

The inductive content analysis using the unconstrained coding matrix revealed the specific manifestations of the cyber affordances by the actors in the sample chats. The codes arising from the specific cyber affordance category are named sub-affordances, addressing RQ1: What form do the chat-based cyber affordances take? The sub-affordances occurring under each category were identified and are presented in Table 3. Examples of the sub-affordances as they occurred in the chats are provided in Appendix 3.

Table 3: Identifying the Use of Cyber Affordances in the Chat Sample

Primary Affordance conceptualization	Occurring Sub-affordances	Description
Cyber ID Expressing and discussing identity-**related parameters**	Name	Discussing actors' names
	Age	Discussing actors' age
	Gender	Discussing actors' gender
	Location	Discussing actors' location
	Social status	Discussing actors' social status
	Nicknames	Discussing actors' nicknames
Cyber Presence Online manifestation of identity-**related parameters**	Photos	Discussing photos
	Videos	Discussing videos
	Voice/call	Discussing calls or voice messages
	Platforms	Discussing digital platforms
	Links	Discussing links
	Texts	Discussing texts
Cyber Time Online status and a-synchronized online presence	Online status	Discussing online status
	Previous message in chat	Referring to previous in-chat message in the current chat
	Previous call/SMS outside of chat	Referring to previous call/SMS exchanged outside the chat

	Previous meeting experience for both actors	Referring to previous real-life experience for both actors after having met
Cyber Fantasy Abstract image construction (imaginative state) achieved through online text exchange	Explicit Fantasy	Expressing imaginative states with explicit sexual content
	Passive Fantasy	Expressing imaginative states with implicit or non-explicit sexual content
	Suggestive Fantasy	Expressing imposture of an imaginative state, hinting toward passive or explicit imaginative states
	Non-malicious Fantasy	Expressing construction of imaginative states that do not contain explicit, implicit, or suggestive sexual imaginative states. Image construction of miscellaneous nature
Cyber Synchronization Toward stability and assessing the potential of practicing imaginative states (leveling of the minds of the actors in the communication)	Seeking Approval	Seeking approval toward an imaginative state/a request toward imaginative state usually expressed as a question that invites construction of an imaginative state
	Expressing Approval	Expressing approval toward an imaginative state, usually expressed as compliance, agreement, or confirmation to seeking approval, or a stand-alone positive statement relating to the image-creation invitation
	Neutrality	Neutrality, doubt, or insecurity regarding the construction of imaginative states, usually expressed neither as compliance nor as image invitation, but a neutral statement toward the imaginative state discussed
	Dismissal	Dismissal of, or non-compliance with, the imaginative states discussed or asked, denying construction of imaginative states
	Mirroring	Complete agreement between two constructed imaginative states between the actors
	Manipulation	Construction of an imaginative state aimed at changing one's attitude toward another imaginative state, usually expressed as a compliment,

Cyber Synchronization (Continued*)		suspenseful reaction, and "sugar-coating"
	Imperative/Force	Imperative imposture of an imaginative state/a command for adopting a suggested imaginative state, usually expressed as forceful language
	Aggression	Aggressive imposture of an imaginative state/an aggressive command for adopting a suggested imaginative state, usually expressed through threats or insults
	Break of Contact	Constructing imaginative states toward breaking the contact or synchronization, usually expressed as unavailability of further practice of imaginative states or leaving the conversation
	Neutralization	Constructing imaginative states that served to neutralize negative polarization toward the suggested imaginative states within the chat
Cyber Control Evaluating risks for the established relationship or exchanged communication in regard to law enforcement or social control, risk awareness, or trust control	Law Enforcement Control	Discussing law enforcement control in regard to imaginative states or the formed relationship
	Social Control	Discussing social control in regard of imaginative states or the formed relationship
	Risk Awareness	Expressing awareness of the possible negative outcomes of the information exchanged or the general wrongness of the formed relationship
	Trust Control	Evaluation of the risk of disclosure of the discussed imaginative states or the formed relationship

5.2 Theme dynamics

The conceptual model depicted cyber affordances that might guide the offender's and victim's paths around the cyber-grooming themes presented in Section 3. In this study, I first coded each message to the theme to which it belonged (using a structured coding matrix in regard of the themes, outlined in Appendix 2), and for each message, I coded which of the Internet affordances were being used (using an unconstrained coding matrix in regard to the affordances, outlined in Appendix 3). In the next section, I present an example of a descriptive analysis of the dynamics between the offender and victim themes used in the same chat. I strive to answer RQ2: How do the offender and victim utilize the cyber grooming themes as the chat progresses? I do this by measuring the frequency of occurrence of the theme codes for each message in STATA, as the chat progressed over time, for a randomly selected chat log from the date set.

The offender in Chat 1 expresses only five themes from the suggested themes in the integrated model (as presented in Appendix 2): introductory messages, assessment, rapport building, CAM, and physical abuse potential (Figure 8). In Figure 8, we see how the offender loops and switches between the themes (each marked with different color) in the natural progression of the chat ("0" – being the first message, and 280 being the last message in Chat 1). The most dominant theme of the offender while grooming the victim in Chat 1 is the assessment theme. This theme is defined as *assessing the individual characteristics of the offender, the individual characteristics of the victim/offender regarding potentiality, while getting to know each other, the environment (location, family, and relationships), willingness and availability, sexuality and sexual experiences*. We also see that the offender is switching heavily between the themes of assessment, rapport building, and physical abuse potential. For example, the introductory messages (red) signify every time the offender and victim start a new conversation (regardless of whether it is on the same or a different date). The most frequently occurring theme in this chat immediately following the introductory messages is the assessment theme. The CAM theme is the least occurring theme in this chat.

In the same chat, the victim mostly responds with rapport-building messages to the offender (Figure 9). Rapport building is defined in the structured coding matrix as *simulating friendship/romance, coordination, predictability, and stability of behaviors.* We also observe a high discrepancy between the offender and victim fluctuation of the themes in the same chat. For example, between the 240th and 280th message in this chat, we see that the offender is persistent in his assessment of the victim (lines 240–280, Figure 8), while the victim replies with messages belonging to the rapport-building theme (lines 240–280, Figure 9).

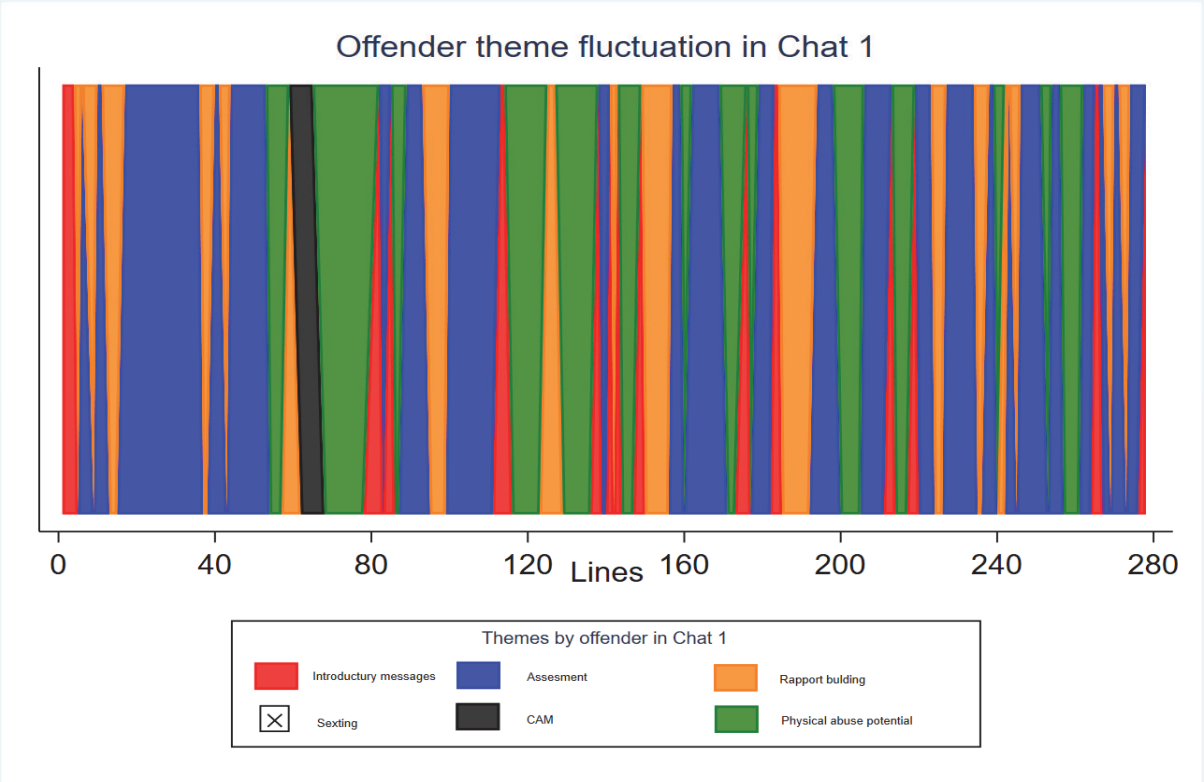


Figure 8: Offender theme fluctuation in chat 1

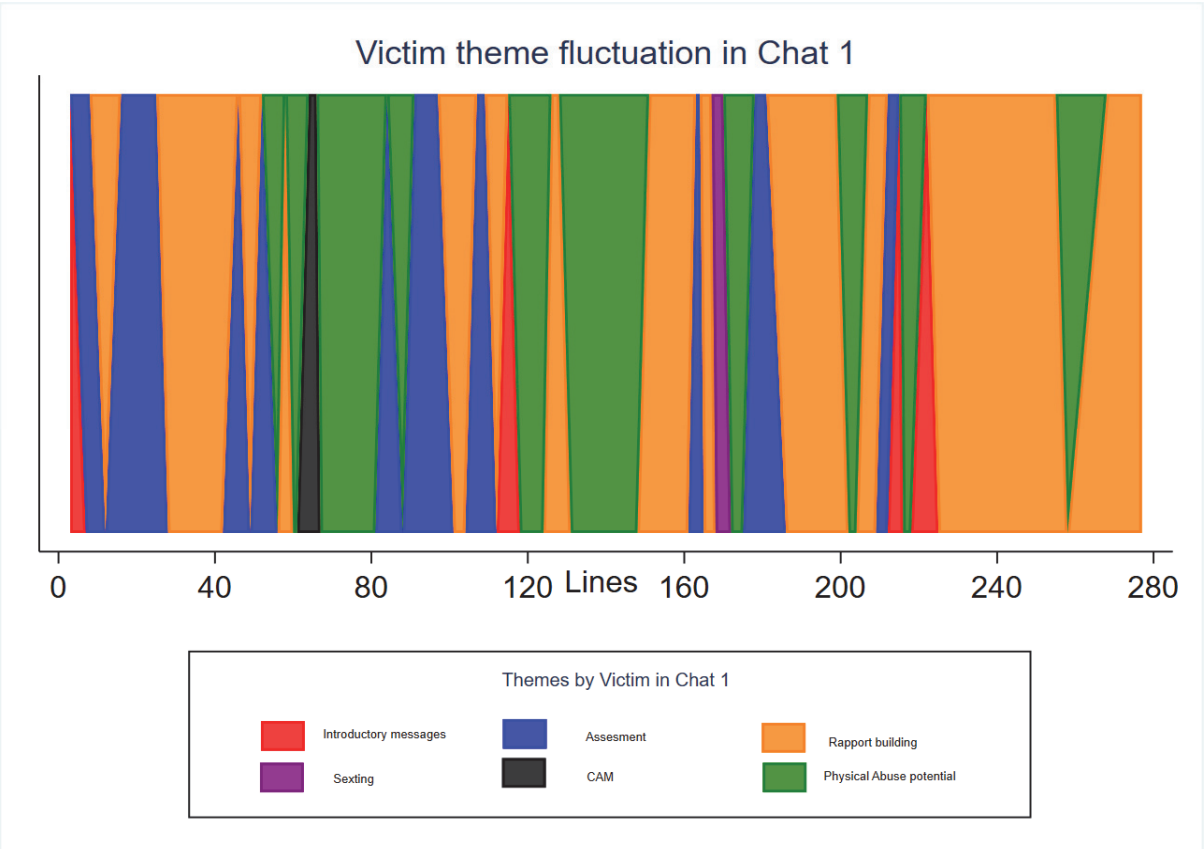


Figure 9: Victim theme fluctuation in chat 1

Regarding the theme fluctuation in relation to the offender and victim, the results show that, most importantly, the offender does not follow a step-by-step progression in the themes while grooming and that there is a tendency to switch and loop between certain themes, perhaps influenced by the victim responses. The victim's "heavy lingering" in a specific theme (in this case, rapport building—orange) suggests a possible misinterpretation of the messages sent by the offender. This mismatch suggests that the victim does not perceive the malicious intentions of the offender (while the offender asks the victim questions assessing her sexual maturity or availability in relation to an older man, the victim shares information as if it were a friendly disclosure to a peer). Such friendly responses from the victim seem to encourage the offender to persist with the assessment theme, which is visible in the offender graph (Figure 8) between the 240th and 280th messages. This theme fluctuation analysis can be highly valuable as a tool in offender-profiling techniques for the purpose of law enforcement prevention. Future research will be able to derivate novel cyber-exclusive offender typologies that can aid in developing offender registries and improve tailored offender psychosocial treatments. Moreover, conducting future explorations in such a manner will help educate victims in terms of which of their behaviors motivate, trigger, and accelerate predatory behavior in offenders. We have thus been educating children against participating in what we have recorded as the most alarming behaviors (sending pictures, revealing location, etc.), yet sometimes, some of the least alarming behaviors could potentially trigger the offender the most. A friendly response from a victim might invite a seemingly non-malicious response from the offender, which only encourages the communication. Advice to youth on how to safely practice and frame these "friendly" responses can make a positive difference in not triggering a potential offender. Moreover, this exploration urges future research on process modelling to consider both actors in the process they attempt to capture in chat-interactive cybercriminal incidents.

5.3 The most dangerous cyber affordances

The descriptive analysis in this section represents an exploration of the most frequently deployed cyber affordances in all the chats, which should reveal the most dangerous cyber affordances. In this endeavor, I answer RQ3: Which of the cyber affordances are most frequently deployed in the chats?

The results show that cyber synchronization (83%) and cyber fantasy (67.3%) were the most frequently used affordances by both the offender and victim in all the chats (Figure 10), thereby suggesting that these affordances are the most dangerous in cyber grooming.

Cyber fantasy is a cyber affordance described as an abstract image construction (imaginative state) achieved through online text exchanges, while cyber synchronization is a cyber affordance described as achieving stability and

assessing the potential of practicing imaginative states (leveling of the minds of the actors in the communication).

In terms of the use of cyber affordances by the offender and victim (Figure 11), cyber synchronization is used more often by the offender (89.2%) than the victim (73.1%), while the victim uses cyber fantasy (71.1%) more often than the offender (64.8%). With marginal differences, the victim uses more cyber time (28.2%) and cyber control (10.3%) than the offender, at 22.8% and 8%, respectively. With slight differences, the offender uses more cyber presence (28.7%) than the victim (25.8%). Cyber identity is almost equally used by the victim (30%) and offender (29.3%).

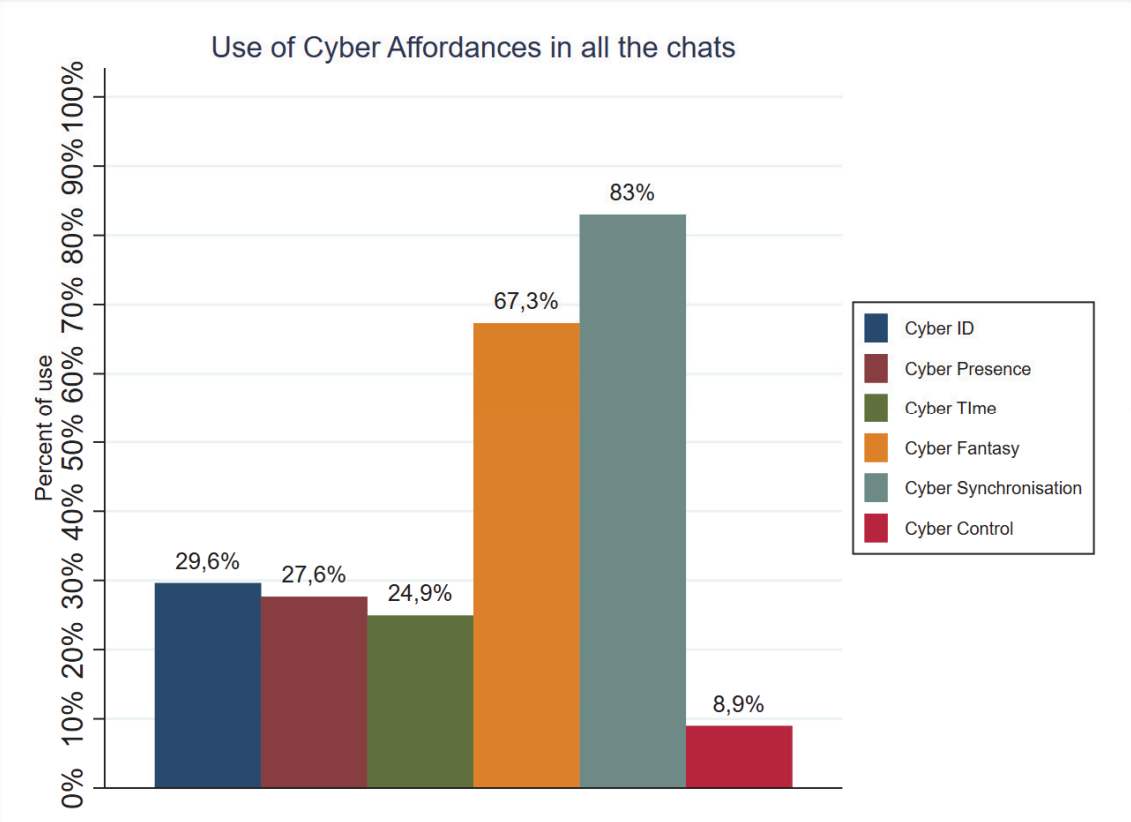


Figure 10: Use of the cyber affordances

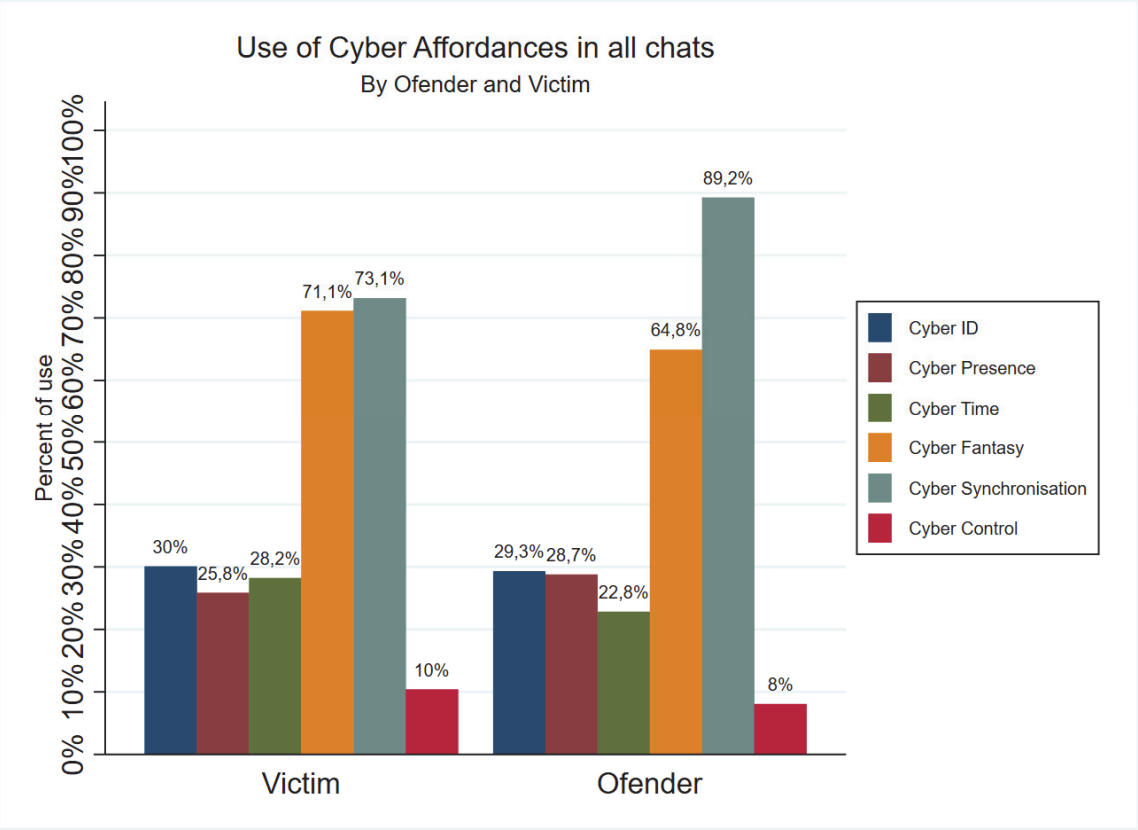


Figure 11: Use of the cyber affordances by the victim and offender

5.3.1 Use of cyber synchronization

The dismantling of cyber synchronization into separately occurring sub-affordances, or states of mind, shows that the most used sub-affordance by both the offender (69.2%) and victim (50%) was seeking approval (Figure 12). The most predominantly used sub-affordances by the offender compared to the victim were seeking approval (69.2%) and manipulation (22.3%), while the most predominantly used sub-affordances by the victim in comparison with the offender were expressing approval (22.1%), neutrality (17.5%), and dismissal (23.3%).

Cyber synchronization seems to be the underlying mechanism that pushes the offender's agenda, while at the same time creating the most significant vulnerability in the victim. The predominant use of seeking approval and manipulation by the offender over the victim likely reflects the predatory and persuasive nature of the offender's agenda. Conversely, the predominant use of expressing approval, neutrality, and dismissal perhaps underscores the vulnerability of the victim. It appears that even though the victim seems to "fight back" with neutrality and dismissal, this does not seem to repel the offender; on the contrary, it fuels his efforts at persuasion.

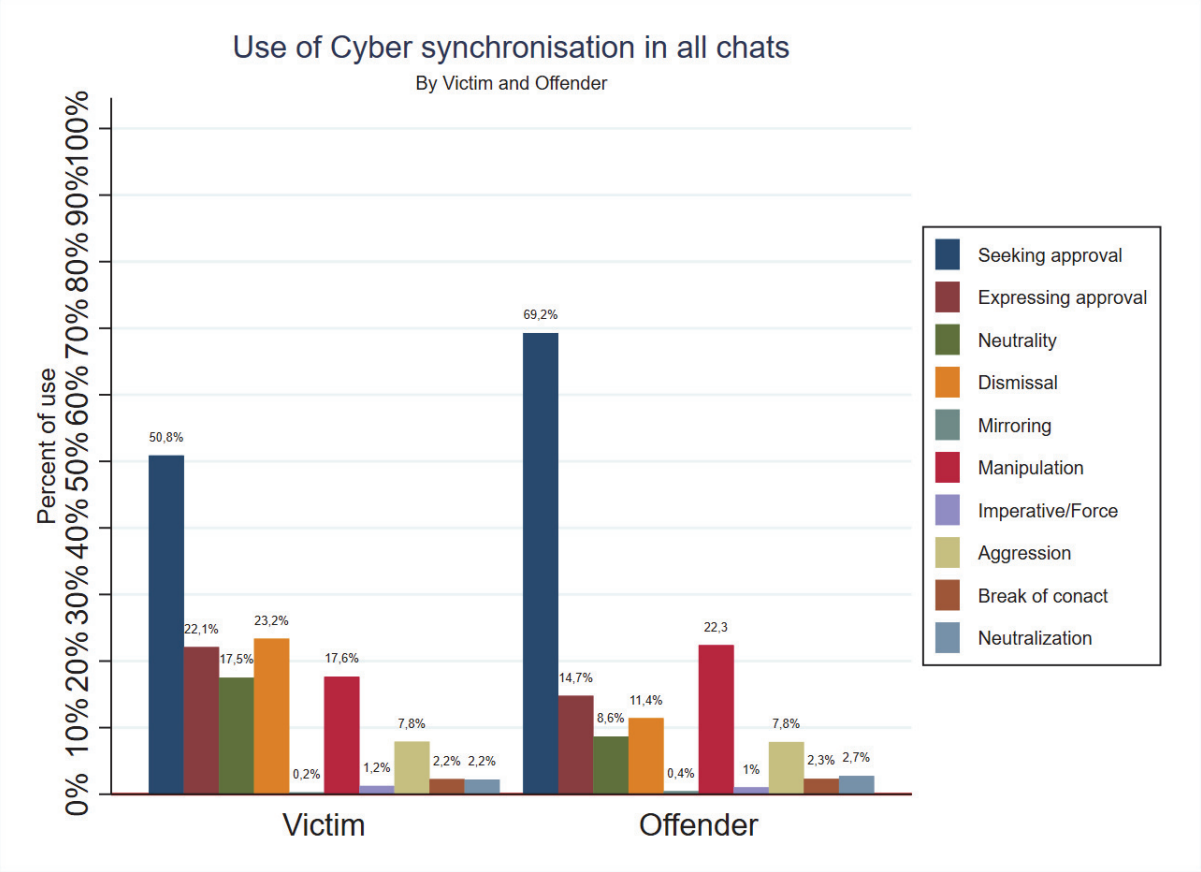


Figure 12: Use of the cyber synchronization by the victim and offender

5.3.2 Use of cyber fantasy

The dismantling of cyber fantasy into separately occurring sub-affordances, or states of mind, shows that, first, the most used fantasy sub-affordance was non-malicious fantasy (62.2% by the victim and 56.9% by the offender), while the least used was explicit fantasy (9.8% by the victim and 7.5% by the offender) (Figure 13). All the cyber fantasy sub-affordances were used more often by the victim than by the offender. This means that the victim used more explicit, passive, suggestive, and non-malicious fantasy than the offender in all the chats.

It might be the case that the offender has a narrow mandate of pushing victims toward critical incidents more exclusively, rather than engaging in fantasy in general, and that the victims believe that they are in a romantic relationship with the offender, which might explain the greater use of fantasy. Again, a closer look at the offender's use of cyber fantasy, in general, is still very high (64.8%), only 8.3% behind the victim.

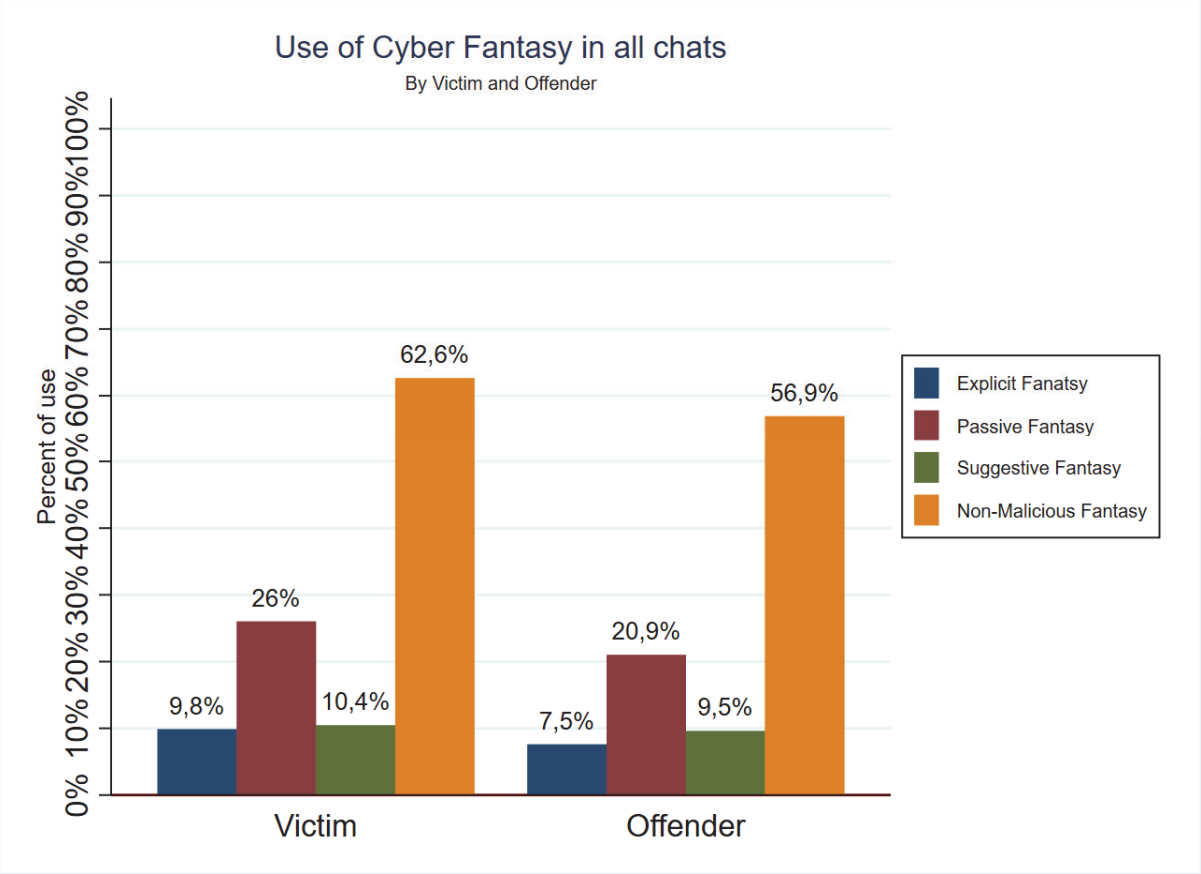


Figure 13: Use of cyber fantasy by the victim and offender

The more worrisome finding here is how the offender and victim engaged with the sub-affordances occurring within cyber fantasy. The most used sub-affordance by both actors was non-malicious fantasy, while the least used was explicit fantasy. Non-malicious fantasy depicts textual image construction of a miscellaneous nature, while explicit fantasy depicts textual, sexually explicit image construction. This means that when cyber fantasy is used as an affordance, both the offender and victim use non-explicit, seemingly non-malicious imaginative states or naive language, which can range from talking about the weather or what they had for lunch to their hair color. Such use of non-malicious imaginative states can be very difficult to detect as alarming by a preventive software or judged as potentially risky by the victim. Explicit fantasy, however, even though it was employed least frequently in the chats, was used mainly by the victim than by the offender. Again, this might have been the case because the offender was more mindful or strategic about using sexually explicit language (either due to his agenda or his awareness of preventive software). However, the victim's initiation of sexually explicit language also speaks of her lack of risk awareness regarding the use of such textual imaginary states. Thus, preventive software design should take into consideration that abusive or sexually abusive language does not occur in all abuse chats.

5.3.3 Use of cyber control

Thus far, I have presented cyber synchronization and fantasy, and their sub-affordances, as the most frequently used affordances by the offender and victim in the chats. However, for the purpose of this thesis, in this section, I also present the cyber control afforance and its sub-affordances, as I believe that the insight it provides is of cruical importance for preventing cyber grooming.

Cyber control is a cyber affordance conceptualized as evaluating the risks of the established relationship or exchanged communication in regard to law enforcement or social control, risk awareness, and trust control. The analysis shows that cyber control was used more frequently by the victim than by the offender, as presented in Figure 14. This affordance consists of the sub-affordances demonstrated within the chats—law enforcement, social control, risk awareness, and trust control—defined as presented in the coding matrix in Appendix 3. From the analysis, we can see that even though these affordances are rarely used in all the chats, the victim shows risk awareness in 6.6% of the chats. The victim is also using law enforcement, social control, and risk awareness more than the offender. There was a slight discrepancy in terms of the offender's predominant use of the trust control sub-affordance compared with the victim's use of this sub-affordance.

Cyber control was the least used affordance in all the chats, yet the most frequently used sub-affordance was the victim's use of risk awareness (depicting expression of awareness of the possible negative consequences of the information exchanged). One would say that this is a positive trend, since risk awareness should repel victims from engaging in such behaviors. However, even though some of the victims expressed such risk awareness and, in some instances, called the offender "pedo" and threatened to report him to the Finnish Net Police, they continued to participate in the communication.

At the same time, the offender was not shy about expressing risk awareness, usually by expressing acknowledgement that he was older than the victim and that the victim was underage. Thus, it seems that the offender's expression of risk awareness served to desensitize the victim to the idea that there is nothing wrong with the age difference, or in some cases, it may even trigger fantasy. Educational practices should further instruct that when something "feels wrong" in a chat, it should be acted on, rather than keeping the communication ongoing.

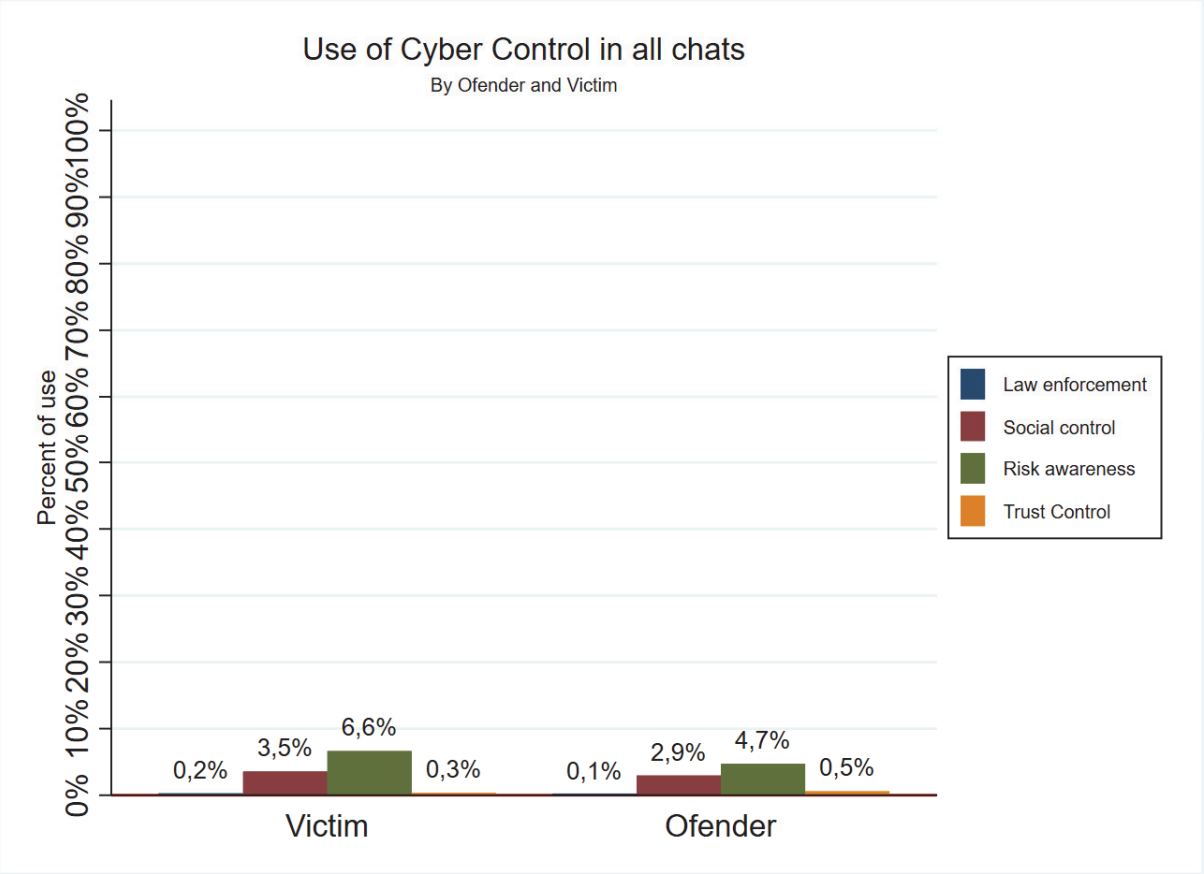


Figure 14: Use of cyber control by the victim and offender

5.4 Cyber affordances and themes

In the next section, I attempt to answer RQ4: To what extent are cyber synchronization, cyber fantasy, and cyber control being used under sexting, CAM, and physical abuse potential themes? I present the use of the selected affordances in these selected themes, as I believe that they are the most malicious themes in the cyber-grooming process.

5.4.1 Cyber synchronization in the sexting, CAM, and physical abuse potential themes

The most predominantly used cyber synchronization sub-affordances by the offender, compared to the victim, in the sexting, CAM, and physical abuse potential themes were seeking approval and manipulation (offender in Figure 15 to 17). However, the victim expressed greater approval (22.7%) and less neutrality (11.3%) and dismissal (11.3%) in the sexting theme than in the CAM or abuse potential theme (victim in Figure 15). We see that as the victim's use of expressing approval dropped in the CAM and physical abuse potential themes

(victim in Figures 16 and 17), the neutrality and dismissal sub-affordance increased (Figures 16 and 17, with the highest increase recorded for dismissal (39.6%) in the physical abuse potential theme (Figure 17). As the victims use of expressing approval dropped, the offender's use of seeking approval increased (most drastically in the CAM theme, 79.6%, in Figure 16), and his use of manipulation increased (most drastically again in the CAM theme, 21.7%, in Figure 16).

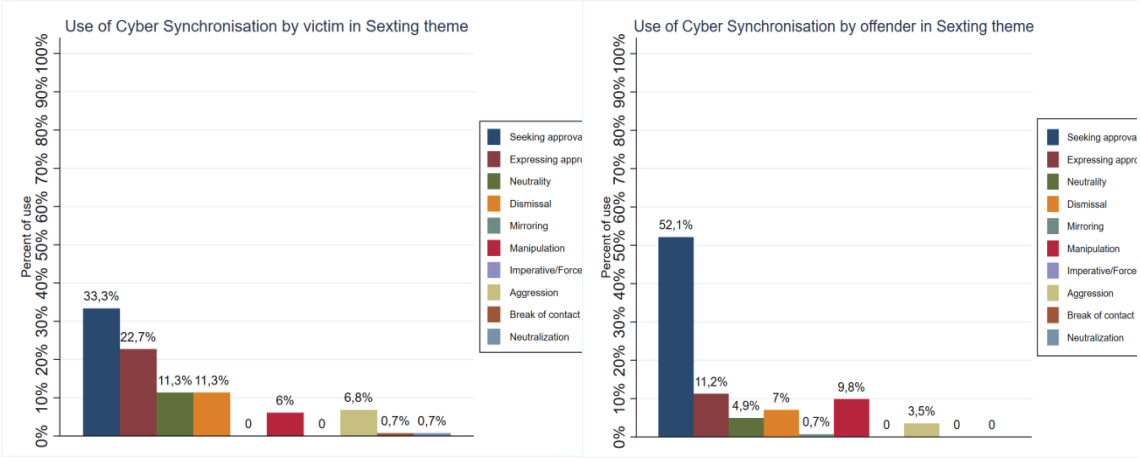


Figure 15: Use of cyber synchronization in the sexting theme by the victim and offender

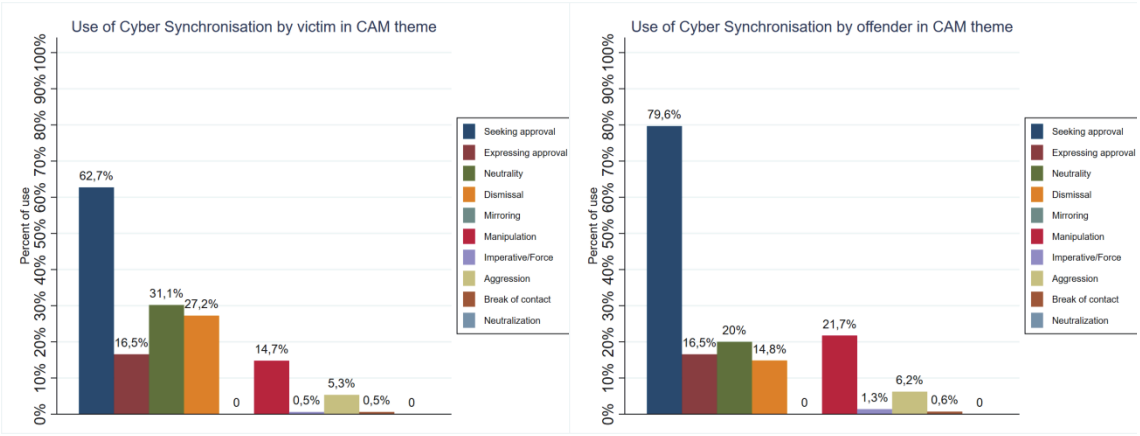


Figure 16: Use of cyber synchronization in the CAM theme by the victim and offender

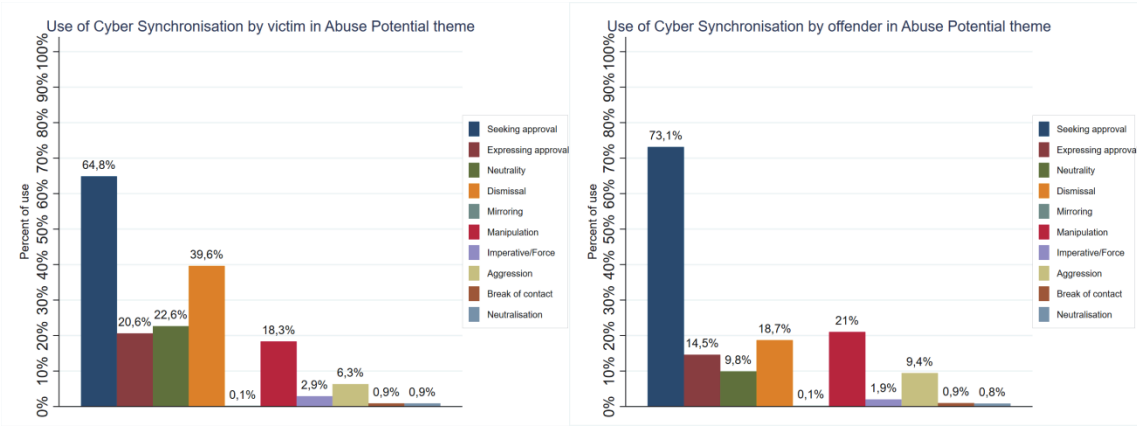


Figure 17: Use of cyber synchronization in the physical abuse potential theme by the victim and offender

The analysis of how cyber synchronization was used in the selected themes shows that the victim was most compliant with sexting. As the victim showed the highest use of expressing approval in this theme, the offender was least engaged in seeking approval. As the victim's use of expressing approval decreased in the physical abuse potential theme and even more drastically in the CAM theme, the use of neutrality and dismissal increased. At the same time, the use of seeking approval and manipulation by the offender rose. This might be further proof that the offender deployed seeking approval mainly as a persuasive technique and that special attention should be given to educating victims about the dangers of sexting and complying with sexting.

5.4.2 Cyber fantasy in the sexting, CAM, and physical abuse potential themes

The trend of the victim's use of cyber fantasy more than the offender persisted in the separate selected themes (victim in Figures 18 to 20). We can see heavy use of explicit fantasy by both the offender and victim in the sexting theme (Figure 18), with a drastic drop in its use in the CAM and physical abuse potential themes (Figures 19 and 20). The second most used cyber sub-affordance by both actors was non-malicious fantasy (Figures 18 to 20).

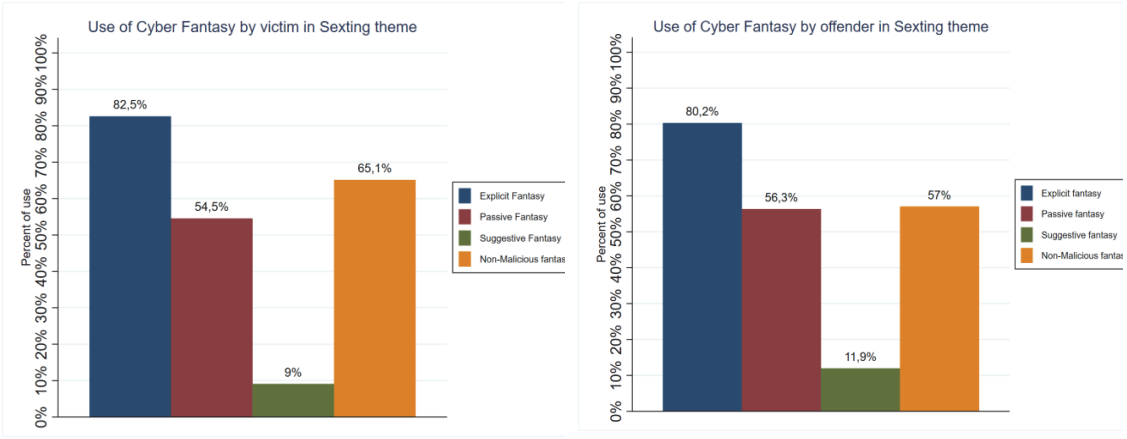


Figure 18: Use of cyber fantasy in the sexting theme by the victim and offender

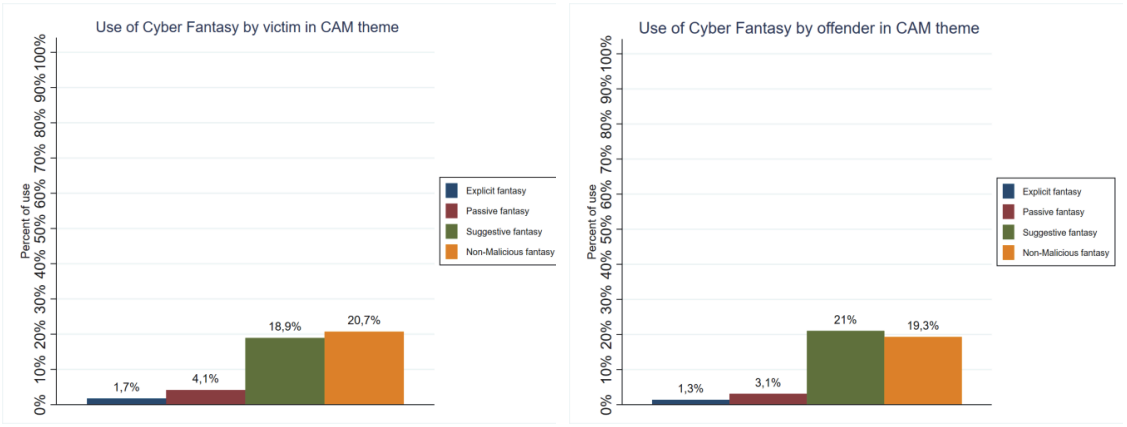


Figure 19: Use of cyber fantasy in the CAM theme by the victim and offender

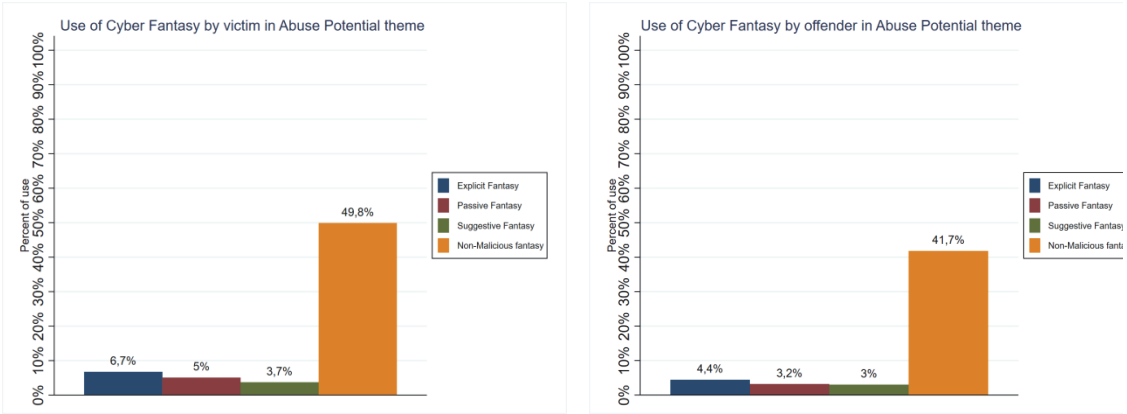


Figure 20: Use of cyber fantasy in the physical abuse potential theme by the victim and offender

The analysis of how cyber fantasy was used in the selected themes shows a drastic drop in the use of explicit fantasy from the sexting to the CAM and physical abuse potential themes. In the context of sexting, one would assume that it would be natural for the actors to make substantial use of explicit fantasy, since sexting as a phenomenon consists of the exchange of sexually explicit imaginative states. However, an interesting insight is the use of the runner-up sub-affordance in the sexting theme, where non-malicious fantasy recorded the most frequent use, and the use of explicit fantasy recorded a drastic drop in the rest of the selected themes. Another interesting finding is that non-malicious fantasy was the most used in the CAM and physical abuse potential themes. This means that even though, during the sexting, the actors used explicit fantasy the most, they also supported these sexually explicit imaginative states with non-explicit imaginative states, i.e., imaginative states where sexual language was not used. It also means that the offender lowered the use of sexually explicit states when he embarked on a quest to procure CAM and suggest a meeting, call, video chat, etc. Perhaps the offender discontinued the use of sexually explicit states in order not to "scare" the victim so that he could more easily reach his goal. Nevertheless, the heavy use of non-malicious fantasy in the CAM and physical abuse potential themes also suggests that the offender was still reliant on imaginative states in persuading the victim. Finally, occurring in the CAM theme, suggestive fantasy was the only sub-affordance that was used predominantly by the offender among all the selected themes. I assume that the trend of the victim using cyber fantasy sub-affordances more frequently than the offender, including, in general, in all the chats, can be interpreted through the victim's innocent approach. The victim does not have a predatory agenda over the offender, so it might have been natural for her to use the chat and connection with the offender to form a regular romantic relationship.

5.4.3 Cyber control in the sexting, CAM, and physical abuse potential themes

The results show a very low use of this affordance in the selected themes by both actors. There is a predominant use of risk awareness (7.6%) by the victim compared to the offender, most significantly expressed in the CAM theme (Figure 22). The use of social control was more significantly expressed in the physical abuse potential theme, where the victim used it more frequently than the offender (8.2%) in Figure 23. Cyber control was used least frequently in the sexting theme by both actors, with a risk awareness use of only 0.7% by both actors (Figure 21).

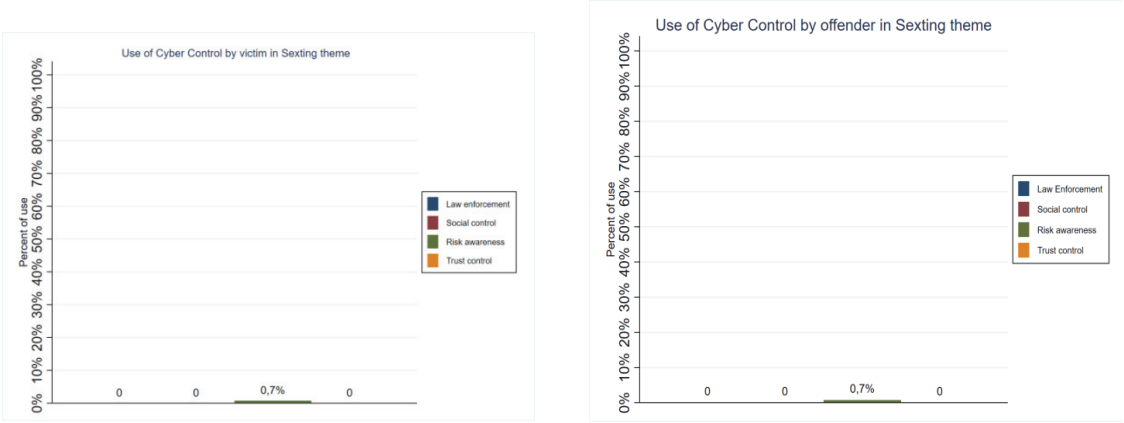


Figure 21: Use of cyber control in the sexting theme by the victim and offender

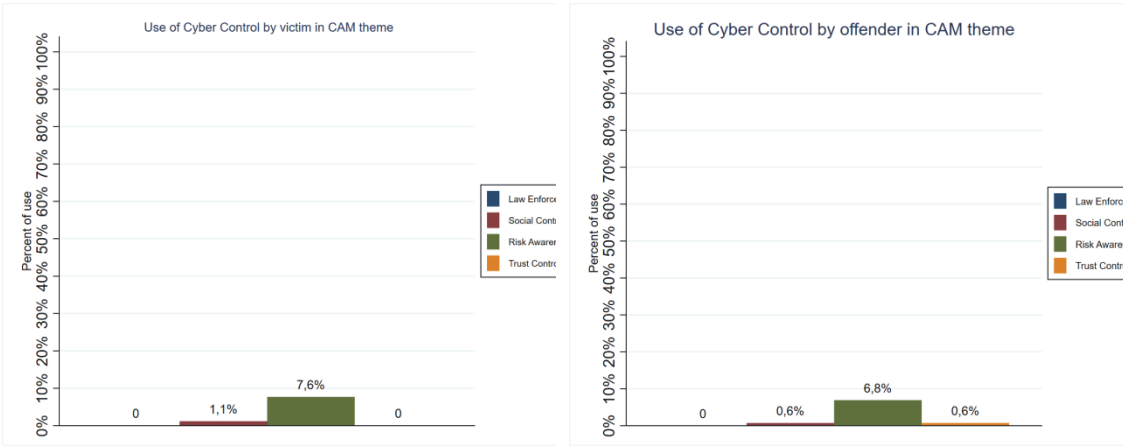


Figure 22: Use of cyber control in the CAM theme by the victim and offender

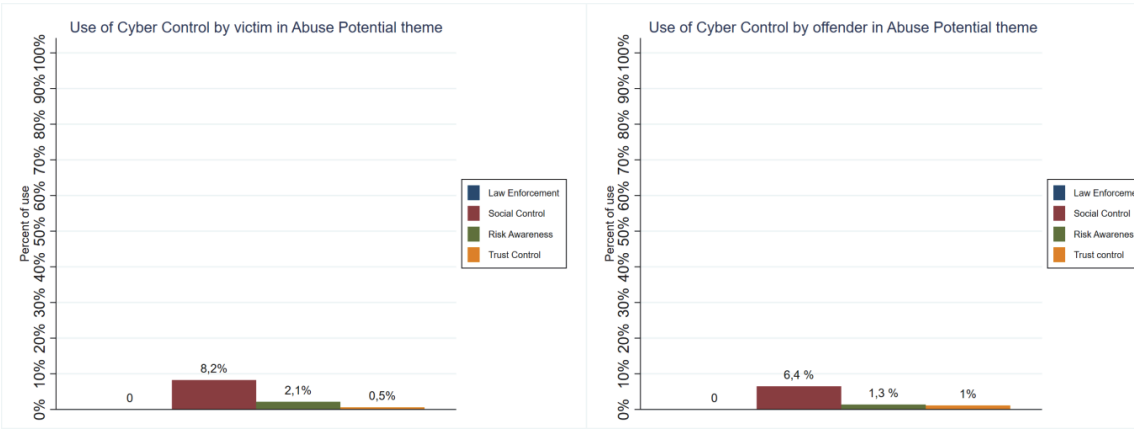


Figure 23: Use of cyber control in the physical abuse potential theme by the victim and offender

The findings regarding the use of the separate cyber control sub-affordances in the selected themes are interesting, not only because of the non-use of the sub-affordances in these themes, which is a finding by itself, but also because of the

sub-affordances used in these themes. The trend that followed is that social control and risk awareness rose within the CAM and physical abuse potential themes, with the highest spike recorded in the use of risk awareness in the CAM theme and the highest spike in the use of social control recorded in the physical abuse potential theme. Both sub-affordances were used predominantly by the victim compared to the offender. Law enforcement was not used at all in these themes, while the use of trust control was minuscule, used only in the CAM and physical abuse potential themes.

These observations confirm that sexting was one of the most applicable themes for both the offender and victim. The victim seemed to show almost no resistance, introducing no law-enforcement or social control and expressing very low risk awareness in comparison within the CAM and physical abuse potential themes. The offender also showed comfort within the sexting theme, without introducing anything within law enforcement, social control, or trust control. According to these themes, the offender seemed to believe that the victim was compliant and that there was no risk of "being caught." A positive trend is that within the CAM theme, the risk awareness seemed to be high, and there was some use of social control (in comparison to the rest of the selected themes), with the victim using these sub-affordances more frequently than the offender. This suggests that the victim demonstrated a level of resistance and an awareness of wrongness. The spike in the use of social control by the victim, compared with the offender, in physical abuse potential signals that while the offender was seeking to assess the potential of physical abuse, the victim's first line of defense was to introduce social control states, either as an excuse for not complying or an implicit threat. The high use of social control by the offender himself, in comparison with the other selected themes, also suggests that he might have felt the need to gain "control over the situation" (in terms of assessing whether social control was present or would be present) as he examined the possibilities for physical abuse.

5.5 Time stamps, affordances, and themes

Earlier in the analysis, I identified four critical incidents occurring in the chats: exchange of calls, exchange of pictures, exchange of live video (streaming), and evaluation of location and meeting potential. These critical incidents were all coded under the sexual abuse theme, and they are potentially the most dangerous actions that can lead to physical abuse or continued online abuse. I strive to answer to RQ5: What information can the cyber affordances and themes provide for evaluating the urgency of physical abuse potential?

I now present a descriptive analysis of these critical incidents in the cases and measure: a) the extent to which the offender requested these critical incidents from the victim; b) the extent to which the victim agreed with the offender's request for the critical incidents; c) the mean days of active conversation before these critical incident offender requests and the victim's agreement occurred; d)

the extent to which the victim requested these critical incidents from the offender; e) the extent to which the offender agreed with the victim's request for the critical incidents; and f) the mean days of active conversation before these critical incident victim requests and the offender's agreement occurred.

The critical incidents are

Critical incident 1 – Calls The results show that in all the cases, the offender requested a telephone call from the victim, while the victim agreed to a call in 47.4% of the cases. On average, the offender requested a call from the victim on the third day of active communication, with the victim agreeing within the fifth day of active communication. Conversely, the victim requested a call from the offender in 15.4% of the cases, with the offender agreeing in 86.6% of the cases. The victim requested a call from the offender on the tenth day, on average, with the offender agreeing to the victim's call request, on average, within the sixth day of communication.

Critical incident 2 – Picture exchange In almost all the cases (97%), the offender requested a picture from the victim, with the victim sending the offender a picture in 88.6% of such cases. The offender requested a picture, on average, on the second day of active communication, while the victim agreed within the eight day of active conversation. In comparison, the victim requested a picture from the offender in 70% of the cases, and the offender agreed to send a picture in almost all such cases (95.1%). The victim requested a picture, on average, on the third day of communication, while the offender agreed to send a picture straight away (including on the third day of communication).

Critical incident 3 – Live video exchange The offender requested a live video exchange (i.e., a Skype call with an active camera) in 90% of the cases, with the victim agreeing in 22.2% of such cases. The offender requested a live video exchange on the fifth day of active conversation, with the victim agreeing, on average, on the sixth day of active conversation. The victim requested a live video from the offender in only 11.2% of the cases, with the offender agreeing to this in all such cases. The victim requested a video exchange, on average, on the 26th day of communication, while the offender agreed to this on the same day of the request.

Critical incident 4 – Assessing location and meeting potential The offender requested the victim's location in all cases, with the victim revealing her location every time. Following this, the offender requested a meeting in the physical world from the victim in almost all the cases (97.5%), and the victim agreed in 62.9% of the cases. The offender requested a meeting from the victim, on average, on the third day of communication, with those victims agreeing to a meeting have done so, on average, within the ninth day of communication. Conversely, the victim inquired about the offender's location in 45.2% of the cases, with the offender revealing his location in all

such cases. Furthermore, the victim requested a meeting with the offender in 51.8% of the cases, and the offender agreed in 93.4% of such cases. Those victims who requested a meeting with the offender did so, on average, on the 17th day of communication, with the offender agreeing on the same day of the request.

The analysis of the critical incidents revealed that, in almost every chat instance, the offender requested a call, picture, live video chat, location information, and a meeting in the physical world from the victim. On average, he made these requests on the third day of active communication. At the same time, the victim recorded the highest agreeable response rates in regard to revealing their location and sending a picture to the offender and the lowest agreement to a video chat. More than half of the victims agreed to a meeting with the offender, and less than half agreed to a call with him. On average, those victims who agreed to the critical incidents did so on the fifth day of communication. The critical incidents observed through the reverse request rate (the victim toward the offender) revealed that the victims were significantly more hesitant about requesting a video or call from the offender, followed by a request for the offender's location, a meeting, and a picture. The offender showed a high agreeable response rate to the victims' requests.

The victim's hesitation in the reverse scenario seemed natural and desirable. In addition, the highest request rate from the victim came from the picture-exchange request. In my opinion, such chat-based requests are often employed when the victim doubts the offender's intentions and wants to make sure that he is really the person he claims to be. At the same time, victims request pictures in order to assess whether the offender is handsome enough when they believe they are in a romantic relationship or show a romantic interest in the offender. Educating children about strategies regarding which identity parameters can be requested from the other actor and in a manner that will discourage predatory behavior can be beneficial.

However, while victims show extreme vulnerability in their willingness to reveal their location and send pictures, they demonstrate the highest resistance to participating in a live video chat. This is an interesting finding. First, it speaks to the need to enhance or reconsider existing[6] educational and prevention material on the dangers of revealing location and sending pictures and the willingness to call or meet strangers from the online world. Second, the victims showed significant resistance to accepting a live video chat. One would assume that the victims would perceive greater risk or feel less comfortable about agreeing to a live video chat than they did in the rest of the agreed incidents. Live video chats might feel intrusive, since they require immediate face-to-face communication with the offender, and victims might feel that they have more

[6] Most awareness-raising campaigns on the dangers of the Internet, in Finland and internationally (some of which I have personally participated in as a facilitator), outline the potential severity of engaging in picture exchanges and revealing location and meeting strangers from the online world.

control in the rest of the incidents, since they can more easily strain or avoid the offender. Future research should be employed in this matter because the repulsive characteristics that the live video chat might possess, which result in victim hesitation, can then be employed for enhancing prevention regarding the rest of the agreed critical incidents.

The critical incident observations also show that the offender was quite straightforward in voicing his intentions (given the short period of three days before reaching the critical incidents) and that the victim, on average, became agreeable towards the requested incident during a period of two days of active communication. Both indicate a shockingly short time gap for possible parental or law enforcement intervention. If such trends persist, with research, we can inform law enforcement and external monitoring systems that they likely have five days in which to intervene from the contact initiation, with the danger of complying with the critical incident by victims peaks between the third and fifth days of communication. This should also inform prevention methods of the importance of intervention before such communication occurs, perhaps in a form of risk awareness or education.

6 DISCUSSION

CGOC is a vivid example of a type of online crime that has its origins in the physical world but that operates very differently from its offline counterpart because of unique behavioral and criminogenic affordances found in the structure and functionality of the Internet. In this dissertation, I attempted to first demonstrate the need for novel ways of studying cyber grooming and cybercriminal phenomena that take place on chat-interactive platforms. The SLRA conducted here outlined major shortcomings in the literature, pointing to the need for a re-conceptualization of how we study cyber grooming. The main propositions for addressing these shortcomings were (1) the need for a cyber contextualization of models/theories that will strive to address cyber grooming in the future and (2) adequate modelling of cyber grooming that would respond to interpersonal and interactive communication.

The conceptual model presented in Section 3 is designed to address these propositions. The theoretical contribution of the model is two-fold. First, it proposed a cyber contextualization of the phenomenon by suggesting an exploration of cyber affordances as conceptual variables that might facilitate cyber-grooming behavior in the online environment. Second, it proposed a way to address the modelling shortcomings of previous literature by including both the offender and victim as interdependent actors in the cyber-grooming process, crucial for studying cyber-contextualized attributes. I now address the implications of these two research prescriptions.

First, "opening the pandorian box" of cyber affordances was a challenging task. Creating cyber affordances as conceptual variables based on Suler's (2004) online disinhibition was an endeavor of disciplined imagination and a hermeneutic exercise. Some might argue that, as a researcher, I have constrained my explorative thought through codes arising in the chats under the conceptual categories of "cyber affordances." One can easily get lost in the context while reading extensive material in a chat form. My instinct in this regard was to follow Walsham (1995) and use these concepts as part of the iterative process of data collection and analysis, since my task was to uncover "cyber-specific" properties within the data. Suler (2004) argued that, when online, a person can shift into an

"intrapsychic constellation" of his physical self and omit the physical selfcharacteristics" (2004, p. 325). Therefore, the major conceptual affordances based on Suler's argument served only as a guide so as not to stray from my original "cyber" explorative task, and the occurring sub-affordances in Appendix 3 are the result of this process.

Critiques on such a "cyber-specific" exploratory approach or the need for new "cyber" theories are generally grounded in the notion that Internet technology is merely a constructed utilitarian extension of human functioning, no different from other socially relevant technological tools (e.g., the telephone; see also Brown, 2006) used in society. This formulation denies the online context of the status of a "separate" world—the argument being that if you are sitting comfortably in your regular physical environment, surrounded by familiar objects, "you are not going anywhere" (Aiken, 2016). Because the processes inherent in the online world are designed by humans for humans, the effects are easily explained by traditional conceptualizations of human motivation, thought, and behavior, including those related to criminality (see Brown, 2006; Grabosky, 2001).

Against this backdrop, some of the occurring sub-affordances from the empirical study (Appendix 3) carry titles such as neutralization and mirroring. I note that these titles do not strictly represent the phenomenon or theory behind the title (e.g., neutralization=neutralization theory, see Copes & Maruna, 2017; mirroring=social learning theory, see Akers, 1973), yet they carry such titles as a sense-making symbol, or representation, of the behaviors found in the chat. Critics might then argue or pose the question, for example, of how different is cyber neutralization from regular neutralization. To answer this, I turn to Greenfeld's (2015) argument that the human brain is a network of neurons that are being shaped, adapted, and evolved by experiences lived and perceived in a given environment. As the "evolutionary mandate" of the human brain is to adapt and thrive, its response to the cyber world as a new environment leads to a unique personalized state of mind that can further result in physical changes to the brain, for better or worse (Greenfield, 2015). Thus, cyber neutralization, for example, might not be categorically different from regular neutralization, although it can be differently manifested in cyberspace.

As the fundamental concept remains that people behave differently as environmental conditions change, when environmental conditions change so radically as to violate the base assumptions of a theory, it seems logical to alter the existing theory or discover new ones to accommodate such change. Therefore, the cyber affordances and sub-affordances, as communicated and found in this thesis, do not exclude the possibility that in a separate research endeavor, they could be explained by complementary theories. Thus, the sub-affordances and their description might be found to be a cyber-specific representation of their correlating explenans of these theories. However, I refrain from further discussing this in this dissertation.

Second, the modelling prescription aims to capture these cyber-contextualized behaviors, or the use of cyber affordances by both actors (the

offender and victim), as they are naturally occurring in the chat in a way that they can influence each other. Such modelling is not novel to the communication literature. One example is IDT (Buller & Burgoon, 1996), which was developed to study deceptive communicative activity in interpersonal face-to-face communication in everyday life. Buller and Burgoon defined deception as a "message knowingly transmitted by a sender to foster false belief or conclusion by the receiver" (p. 205). The deceiving actor must intentionally manipulate or distort the truth to achieve the deceptive goal, while the receiving actor must decide whether to express suspicion of a deception attempt to establish the validity of these messages. From there on, the theory dynamic proposes that understanding deceptive communication requires treating it as an iterative process in which its participants mutually influence each other. IDT has also been applied in studies of online fraud, such as online consumer and e-commerce deception (Grazioli, 2004; Xiao & Benbasat, 2011), social media deception (Tsikerdekis & Zeadally, 2014), and everyday digital deception (Hancock, 2007; Ho & Holister, 2013). To the best of my knowledge, this theory has not been applied to online child sexual abuse techniques. This may be due to general critiques of IDT and its application to online settings. These critiques mainly concentrate on the original theory requirement for a high level of interpersonality, or face-to-face interaction (Grazioli 2004; Tsikerdekis & Zeadally, 2014). In cyberspace, interpesonality in this form is weakened or at least questionable in terms of how it translates webcams, photos, and so on. Its broad application in the grooming literature may also be due to the fact that IDT has been relying on a set of "verbal or none verbal cues that may not all apply to the online world"(Tsikerdekis & Zeadally, 2014, p. 11). These critiques might seem natural, since the original theory was developed, again, for the physical world at a time when Internet interpersonal communication was still in its infancy. However, the application of such a modelling dynamic of including interdependent actors in the communication is beneficial in terms of the specific affordances of the medium in which the communication takes place (Hancock, 2007; Tsikerdekis & Zeadally, 2014). Employing cyber affordances as a form of cyber contextualization to such modelling seems highly desirable.

The empirical contribution of this dissertation is twofold: (1) to demonstrate the potential of studying chat-interactive cybercriminal phenomena in this manner and (2) to produce specific implications in particular domains of action (Walsham, 1995). To achieve this, the dissertation examined this phenomenon in its natural setting through real-life cyber-grooming cases. From a researcher's perspective, this is a great privilege, responsibility, and research impetus. The empirical analysis resulted in worrisome, albeit extremely valuable, results.

Older conceptualizations of cyber grooming have estimated that the grooming process can last a long time before the occurrence of critical incidents or that the offender will achieve critical incidents by gradually desensitizing the victim to the incident of interest (Choo et al., 2009; Leander, Christianson, &

Granhag, 2008; McCarthy, 2010). Older conceptualizations have also posited that a groomer's behavior can be captured in step-by-step explanations or stage theories (Barber & Bettez, 2014; Black et al., 2014; Hui et al., 2015; Kloess et al., 2014, 2015; Miah et al., 2014; Michalopoulos et al., 2014; O'Connell, 2003; Pranoto et al., 2015). The results of the dissertation demonstrate the evolution of cyber grooming, whereby critical incidents can be requested and agreed to unexpectedly in a very short time frame from the initiation of the communication. It also presents the offender and victim as having very dynamic and interdependent behaviors, which is difficult to be captured by stage explanations. Such impulsiveness and dynamics might be due to the evolutionary nature of the Internet and its general embeddedness in today's social and communicative relationships. The Internet has certainly increased the cognitive load in humans, which is recognized in the educational psychology and social cognition literature as the extent to which increased information interferes with information processing (see Chaiken & Trope, 1999; Gilbert et al., 1988; Pass et al., 2003; Sweller, 2011). Higher cognitive loads drive people to resort to more automated processing of information. The greater the cognitive load, the more people use simple heuristics and cognitive shortcuts to make decisions (Fiske & Neuberg, 1990). This is adaptive: It allows people to respond to social cues and make speedy judgments. However, it can also lead to errors in judgment or facilitate offending. Under conditions of high cognitive load, people rely more on intuition, emotion, entrenched beliefs, and reflexive judgement. This can lead to short-cut decision-making processes (see Kahneman, 2003), such as racial stereotyping (Fiske & Taylor, 2017), increased aggression (Topalli & O'Neal, 2003; Topalli & Wright, 2013), and impulsive decisions (see Dorman et al., 2018; Schachar & Logan, 1990).

Such vulnerabilities are especially pronounced in children. Despite the ability of children to adopt, use, and maneuver technology and the Internet for constructive purposes, their decision-making processes while in such environments are limited by their early stage of cognitive development (see Casey et al., 2005; Crone & Steinbeis, 2017). This makes them vulnerable to predatory adults who, as with other types of offenders, are able to selectively incorporate characteristics of the (online) environment into their targeting of victims and use superior knowledge, experience, and social engineering techniques to take advantage of them. Future research should engage in developing best practices for educating children on mindful Internet decision-making in their early stages of cognitive development.

Cyber synchronization and cyber fantasy appeared to be the most frequently deployed among the offender and his victims and were, therefore, deemed most dangerous in the cyber-grooming cases. There have been various typologies in the cyber-grooming literature regarding cyber-grooming offenders, some of which divide offenders into contact-driven or fantasy-driven categories (Briggs, Simon, & Simonsen (2011). Although this particular offender was contact-driven, he continued to use cyber fantasy as the second most used affordance in all chats. I do not believe that there can be a strict line between

contact- and fantasy-driven offenders. In this offender, we saw that the explicit fantasy could even be a result of the actual meeting with the victim. I also believe that almost every online communication possesses imaginative states. How one activates that fantasy might depend on the their motives and vulnerabilities, easily captured by cyber synchronization. Indeed, the results demonstrated that cyber synchronization was the most frequently employed cyber affordance, yet it might be that some of the occurring sub-affordances were tainted by the offender's ill-intended motives and the victim's vulnerabilities. Future research on cyber synchronization in non-malicious chat environments will be highly beneficial for refining malicious cyber synchronization. This also follows for the remainder of the affordances.

A summary of the detailed recommendations for future research and practice deriving from an interpretation of the results can be found in Table 4. When reading these recommendations, I urge readers to be mindful of the small sample size of this study and consider the recommendations with care in terms of the limited generalizability of the findings in regard to this sample size. The recommendations for practitioners should be applied to the suggested target group (law enforcement, social control actors, policymakers or youth, etc.) with careful consideration of the recommendation in consultation with the relevant stakeholders and expertise in regard to the suggested target group.

Table 4: Summary of Recommendations

Recommendations for future research:
1. Future research design and modelling of predatory online communication should consider the victim's input and how this affects the offender's decision-making.
2. Future research on interactive criminal scripts for chat-interactive cybercriminal incidents can be beneficial.
3. Future research could study which forms of natural language by the victim have successfully dismissed or repelled the offender's predatory intentions.
4. Future research can study which forms of natural language that do not contain sexually explicit content are used for highly predatory aims.
5. Future research can study non-sexually explicit "imaginative states" and/or "abstract imaginative information" from victims and its effect on offenders. For example, in which way can non-sexually explicit conversations stimulate predatory behavior in offenders?
6. Properly assessing cyber identity could repel predatory behavior. Future research can study whether victims who insisted on assessing the potential offender's identity (requesting social media links for their personal profile, proof of age) have successfully repelled the offender.
7. Future research should explore in greater detail neutralization techniques initiated at the victim.
8. Future research with access to victimized youth could study victims who were explicitly aware that they were being abuse. Such research could seek to uncover why these victims continued communication with the offender.
9. Future research should engage in developing best practices for educating children on mindful Internet decision-making in their early stages of cognitive development.

Recommendations for practice:
1. Law enforcement and social-control actors have extremely short windows in which to intervene. The results from this sample show that it is very likely that a critical incident will occur in the first five days of communication. Youth, law enforcement, and social-control actors can be advised that it is likely that the predatory intention might peak between the third and fifth day of communication. Preventive educational material can provide youth with tools to develop a risk assessment or defense mechanism to assess their potential risk to predatory behavior prior to their decision to engage in communication.
2. Besides educational instructions to youth and social-control actors of the dangers of the most alarming online practices (such as sexting, sending pictures, location revelation, etc.), there is a need to increase awareness of how descriptive responses to various aspect of everyday life (or any friendly response) can trigger predatory behavior from the offender. Youth can be educated on these descriptive responses as "imaginative states" and/or "abstract imaginative information" as online communicative behavior that creates an image for the communicative party, which might trigger a predatory response in a party with predatory intentions. For example, a potential victim talking about going to the sauna might trigger a naked-body image to the predatory actor in the communication.
3. Youth and social control actors can be advised that simply dismissing or ignoring a critical incident request by an offender could be insufficient in repelling the offender's intentions. On the contrary, it might encourage further persuasion and neutralization aimed at the victim. Such repeated persuasion and neutralization directed at the victim over time could eventually lead to the victim complying with the initially dismissed or ignored request.
4. Youth could be advised that threatening to report an offender to law enforcement or social-control actors would not always repel the offender. On the contrary, threatening to report but not actually reporting, and continuing to engage with the same offender after such threat, could encourage the offender. It might signal to the offender that he/she has succeeded in creating a predatory "safe space" where the victim, even though aware of the wrongness of the communication, has not preventively acted upon it, thus serving as tacit victim compliance.
5. Preventive software developers and research on detecting predatory communication can be advised to also incorporate the detection of predatory natural language processing that does not include sexually explicit language.
6. Youth, law enforcement, and social-control actors can be advised that not all offenders would lie about their age or represent themselves as the victim's peer. Offenders can also misinform the victim by underrepresenting their actual age, which can also be over 18. The victims in this sample did not refrain from continuing contact, even though they knew the offender was an adult. Youth can be advised that even if someone presents themselves as slightly older than the "allowed" age, they could still be misrepresenting their much older age.
7. Youth, social-control actors, and law enforcement might be alarmed at the fact that groomers also use their predatory techniques to recruit other potential victims from their initial victim contact. They might do so by enquiring from their initial victim the age, social media links, and nicknames of the peers of the initial victim.
8. From the sample, it is evident that victims easily engage in sexting. Youth of age 14 and younger can benefit from enhanced prohibitory education on sexting,

	with an age-appropriate gradual introduction of safe online sexuality. Youth of age 14 to 18 can benefit from future preventive educational material in a manner that would promote practicing safe online sexuality, rather than prohibitory prevention measures.
9.	Educational practices and policies that would enhance trust between youth and social-control actors toward everyday disclosure of their online lives can be beneficial.

To conclude this section, I believe that the results of the methods employed in this dissertation have demonstrated a novel way of studying chat-interactive cybercriminal incidents and their potential. First, this dissertation illustrates a way of discovering cyber-specific variables that can be implemented within various online phenomena, which can produce cyber contextualization and cyber-contextualized theory or explanation. A researcher can then pick any chat-interactive cyber phenomenon and try to look for cyber affordances deriving from the theoretically sampled data. Second, it demonstrates the valuable information to be gained if such "3D"modelling is applied. By "3D," I mean a model that studies chat-interactive phenomena while also looking at input from both the offender and victim, as demonstrated through the cyber-specific manifestations of their behavior and the ensuing outcomes.

6.1 Contribution to information systems theory and the IS discipline

This research firmly supports Lee (2001, p. 3) in stating that other disciplines are, at best, contributing disciplines in the IS field. It also answers Baskerville and Myers' (2002) call for IS scholars to widen their perspective to study IS phenomena that will attract broader audiences from the scientific community.

Other disciplines are engaged in work on developing an explanation and understanding of various cyber phenomena from their domain, such as psychological, social, or criminological theories of user behavior. One way in which IS could prove and build its reputation as a firm-standing discipline, offering knowledge and contributions to other disciplines, is to measure and theorize how and why the Internet affects the psychological and social variables studied in reference theories/disciplines.

Further, I strongly believe that this kind of research design should also be considered as a research method by IS scholars. The proposed model is an attempt at measuring concepts such as cyber presence and cyber fantasy, and while it is a demanding and very fresh frontier, we should not forego the challenge. Importantly, other disciplines might argue that online child abuse is a psychological or criminal phenomenon, as they only consider the effects of the psychological or criminological variables that lead to the outcome. However, with this research, the IS discipline can argue that online child abuse is also an IS phenomenon. The psychological and criminological variables that facilitated the

outcome would not have been so successful if the Internet was not a factor in the abuse process. Even if future testing of the idea disproves it, if efforts by other disciplines regarding cyber phenomena operate without knowledge of how the Internet has distorted their disciplinary unit of analysis, the result may be wrong conclusions or unanswered questions.

Ultimately, this type of exploration will open an IS scholarly discussion toward taking a united stand on how IS should recognize concepts that could provide answers to cyber phenomena, which have thus far been answered by reference theories. As previously discussed, online communication passes through the Internet mechanism with or without maleficent characters. By using this type of research to exemplify how to measure Internet characteristics through the stages of a phenomenon, it can further be applicable to measuring other cyber phenomena through their own stages, which could contribute to developing better and stronger IS security polices and service designs.

6.2 Contribution to practice

From the analysis, we learned that enhanced prevention education material should be developed in regard to the dangers of sexting. We also learned that cyber ID and presence affordances can be thought of as being practiced in a manner that can validate the identity of the offender or at least as a means to repelling the offender from pursuing communication. Impulsive or rash decision-making in online environments increases the risk of victimization.

Education on mindful Internet decision-making should also be employed in very early stages of cognitive development. Developing children's intuition in terms of detecting risk awareness and manipulative, neutralizing, and aggressive behaviors from potential offenders can increase the reporting prevalence of deviant or criminal cyber phenomena to law enforcement and parents. Efforts should also be put into developing trust between victims and their social environment so as to encourage disclosure of such online experiences. Youth should also be instructed on the forms of malicious online communication that does not possess, for example, alarming precursors or cues of explicit fantasy. Educating youth that communication in the form of non-malicious fantasy can be highly beneficial. Some offenders do not use explicit sexual language in their abusive and predatory scripts and modus operandi. Any friendly response or image construction from the victim can trigger the offender's most coercive behaviors. Future research on identifying the natural language in such "friendly responses" that have triggered explicit fantasy in offenders can construct novel educational materials for safe Internet practice.

This dissertation demonstrates how extensive research can be highly beneficial for enhancing law enforcement prevention. The most alarming results were that, on average, there are only three days between the initiation of the contact and critical incident requests from the offender and two days before the victim agrees to the critical incidents. Preventive software and law enforcement

prevention methods should be aimed at timely prevention. Research on detecting chat-message time-stamp intervals and frequencies in relation to critical incidents can provide solutions for timely law enforcement prevention. Furthermore, extensive research on the offender's theme fluctuation can be used to develop registries and pools of offenders for law-enforcement flagging systems. Preventive software that deals with natural language processing and detection should be developed and used in training in a manner that will detect non-explicit sexual language as well as language aimed at recruiting potential victims via a current victim. Research efforts should be employed for natural language processing in relation to the above-stated cyber affordances.

6.3 Limitations

The results of the empirical study are based on studying one offender and his fourteen victims. The fact that the offender does not vary in terms of the victims can be limiting in terms of generalizing the results to the offender population. However, I believe that having one offender and varied victims can also be an asset in deriving conclusions regarding offender behavioral patterns and how victim variation might influence those patterns. We can see this, for example, when the victims did not comply with meeting the offender, he switched to heavily pursuing calls or discussing the recruitment of other victims who would like to meet him. Nevertheless, future research should replicate this study, though with a larger pool of offenders.

7 CONCLUSION

CGOC and its dynamics do not occur solely as technology-enabled crime or deviant human behavior; instead, it occurs when technology and deviant human behavior interact through the (miss) perception of information.

This dissertation proposed a novel way of studying chat-interactive cybercriminal incidents through a discovery of cyber affordances as cyber-specific conceptual variables, which the offender and victim use during the cyber-grooming process.

The theoretical contribution of this dissertation encourages researchers to study cyber-specific variables for different cyber phenomena of interest and provides a methodological example of how to perform such research. Information technology has already been unshackled from its physical grounding. We can literally say that it is all up in the *cloud*. I argue that researchers should follow, but not abandon, and unshackle themselves from previous knowledge tied to the physical world and move toward independent explorations in the Cyber World.

With today's widespread Internet usage at an increasingly younger age and access to the Internet, in general, whereby it is even debated as a human right, it seems impossible to limit usage or present preventive strategies that will promote banning access to certain content or limiting access to information and social media connections. The practical contributions of the thesis do not condemn or limit Internet usage and its benefits; rather, it promotes safe practice.

With this kind of research, I strive to propose new ways of safe Internet behavior by highlighting the Internet's most seductive and dangerous aspects. Learning from cyber-grooming chat transcripts, I saw the grave result of using the most beneficial characteristics of the Internet in a malicious or unsafe manner, creating the opportunity to discover possibilities of how to minimize the risk created by the internet and promote their safe practice.

SUMMARY IN FINNISH

Lasten seksuaalinen nettihoukuttelu mahdollistuu verkkoympäristössä. Rikoksen taas toteuttaa ihminen, jolla on psykologisia ominaisuuksia, jotka mahdollistavat tällaisen rikoksen. Kuitenkin seksuaalisen nettihoukuttelun ymmärtämisessä on hedelmällisintä yhdistää verkkoteknologian mahdollistama informaation muokkaaminen ja rikoksentekijän mieleen liittyvän vuorovaikutuksen tarkastelu sen sijaan, että tarkasteltaisiin näitä ilmiöitä toisistaan erillään.

Tässä väitöstyössä esitetään kokonaan uusi tapa tutkia seksuaalista nettihoukuttelua tutkimalla hyväksikäyttäjän ja uhrin välistä keskusteluseksenssiä ja siinä havaittuja verkkoympäristön tuottamia erityisiä mahdollisuuksia (affordansseja) yhdistämällä niitä samassa prosessissa esiintyviin käsitteellisiin muuttujiin. Teoriaa sovelletaan todelliseen netissä tapahtuneeseen hyväksikäyttötapaukseen, jota analysoidaan kehitetyn teorian valossa. Tulosten pohjalta esitetään suosituksia sekä tutkimusta että käytännön rikostorjuntaa varten.

Tämän kaltaista seksuaalisen nettihoukuttelun keskusteluanalyysiä hyödyntävä tutkimus voi edistää netin turvallista käyttöä ja valaista pahimpia käytön vaaroja. Tutkimuksessa on esitetty malli, jossa tutkitaan verkkoteknologian avulla tapahtuvaa tiedon muokkausta ja rikoksen tekijän ja uhrin verkkovuorovaikutuksessa havaittuja toimintamahdollisuuksia. Malli voi luoda uusia metodologisia tapoja tutkia verkkorikollisuutta laajemminkin. Uudenlaiset tutkimuksen ja verkkorikosten estämisen näkökulmat ovat tarpeen, koska internetin käytön tai sisällön rajoitukset ovat nykypäivänä hankalasti toteutettavissa. Lisäksi yhä nuoremmat lapset käytävät internetiä. He ovat varsin haavoittuvia tällaisten rikosten edessä.

Informaatioteknologia ja siihen liittyvä verkkoteknologia on jo paljolti fyysisen maailman lainalaisuuksista irrallaan. Myös tutkimuksessa tulisi huomioida ilmiöiden muuttuminen kyberilmiöiksi ja tarkistaa aiempia fyysiseen maailmaan sidottuja teorioita, uudelleen arvioida niitä ja sovittaa niitä verkkoympäristöihin. Tämä tulisi huomioida myös rikoksentorjuntaan liittyen ja kehittää tietoa ja käsitteistöä vastaamaan paremmin tietoverkoissa tapahtuvia psykologisia ja sosiaalisia ilmiöitä.

REFERENCES

Acar, K. V. (2016). Sexual extortion of children in cyberspace. *International Journal of Cyber Criminology, 10*(2), 110–126.

Agustina, J. R. (2015). Understanding cyber victimization: Digital architectures and the disinhibition effect. *International Journal of Cyber Criminology, 9*(1), 35–54.

Aiken, M. (2016). *The cyber effect: An expert in cyberpsychology explains how technology is shaping our children, our behavior, and our values--and what we can do about it*. New York: Spiegel & Grau.

Aslan, D., & Edelmann, R. (2014). Demographic and offence characteristics: A comparison of sex offenders convicted of possessing indecent images of children, committing contact sex offences or both offences. *Journal of Forensic Psychiatry and Psychology, 25*(2), 121–134.

Bandara, W., Miskon, S., & Fielt, E. (2011). A systematic, tool-supported method for conducting literature reviews in information systems. *Proceedings of the 19th European Conference on Information Systems (ECIS)*. June 9–11, 2011, Helsinki, Finland.

Bandura, A. (1989). Human agency in social cognitive theory. *American Psychologist*, *44*(9), 1175-1184.

Barber, C. S., & Bettez, S. C. (2014). Deconstructing the online grooming of youth: Toward improved information systems for detection of online sexual predators. *Proceedings of the 35th International Conference on Information Systems: Building a Better World Through Information Systems* (pp. 1–20). Atlanta, GA: Assocoation of Information Systems.

Baron, R. M., & Kenny, D. A. (1986). The moderator–mediator variable distinction in social psychological research: Conceptual, strategic, and statistical considerations. *Journal of Personality and Social Psychology*, *51*(6), 1173-1182.

Baskerville, L. R., & Myers, D. M. (2002). Information systems as a reference discipline. *MIS Quarterly, 26*(1), 1–14.

Bates, A., & Metcalf, C. (2007). A psychometric comparison of Internet and non-Internet sex offenders from a community treatment sample. *Journal of Sexual Aggression, 13*(1), 11–20.

Beard, K. W. (2005). Internet addiction: A review of current assessment techniques and potential assessment questions. *CyberPsychology & Behavior, 8*(1), 7–14.

Bernhard, E., Recker, J. C., & Burton-Jones, A. (2013). Understanding the actualization of affordances: A study in the process modeling context. *Proceedings of the 21st International Conference on Information Systems (ICIS)*. June 5–8, 2013. Utrecht, the Nethelands.

Bhattacherjee, A. (2012). *Social science research: Principles, methods, and practices*. (Textbooks Collection, 3). Retrieved from http://scholarcommons.usf.edu/oa_textbooks/3

Biderman, A. D., & Reiss Jr., A. J. (1967). On exploring the "dark figure" of crime. *The Annals of the American Academy of Political and Social Science, 374*(1), 1–15.

Black, P. J., Wollis, M., Woodworth, M., & Hancock, J. T. (2014). A linguistic analysis of grooming strategies of online child sex offenders: Implications for our understanding of predatory sexual behavior in an increasingly computer-mediated world. *Child Abuse & Neglect, 44*, 140–149.

Block, J. J. (2008). Issues for DSM-V: Internet addiction. *American Journal of Psychiatry, 16*(5), 306–307.

Boell, S. K., & Cecez-Kecmanovic, D. (2014). A hermeneutic approach for conducting literature reviews and literature searches. *Communications fo the Association of Information Systems, 34*(12), 257-286..

Briggs, P., Simon, W. T., & Simonsen, S. (2011). An exploratory study of Internet-initiated sexual offenses and the chat room sex offender: Has the Internet enabled a new typology of sex offender? *Sexual Abuse*, 23(1), 72–91.

Brown, S. (2006). The criminology of hybrids: Rethinking crime and law in technosocial networks. *Theoretical Criminology*, 10(2), 223–244.

Buller, D. B., & Burgoon, J. K. (1996). Interpersonal deception theory. Communication theory, 6(3), 203-242.

Button, M., Nicholls, C. M., Kerr, J., & Owen, R. (2014). Online frauds: Learning from victims why they fall for these scams. *Australian & New Zealand Journal of Criminology, 47*(3), 391–408.

Cano, A. E., Fernandez, M., & Alani, H. (2014). Detecting child grooming behaviour patterns on social media. In: SociInfo 2014: *The 6th International Conference on Social Informatics, 10-13 Nov 2014, Barcelona, Spain*

Casey, B. J., Tottenham, N., Liston, C., & Durston, S. (2005). Imaging the developing brain: What have we learned about cognitive development? *Trends in Cognitive Sciences, 9*(3), 104–110.

Cecez-Kecmanovic, D., Galliers, R. D., Henfridsson, O., Newell, S., & Vidgen, R. (2014). The sociomateriality of information systems: Current status, future directions. *MIS Quarterly, 38*(3), 809–830.

Chaiken, S., & Trope, Y. (Eds.). (1999). *Dual-process theories in social psychology*. New York: Guilford Press.

Choo, K. K. R. (2009). Online child grooming: A literature review on the misuse of social networking sites for grooming children for sexual offences. AIC Reports: Research and Public Policy Series, 103. Canberra: Australian Institute of Criminology.

Chou, C., Condron, L., & Belland, J. C. (2005). A review of the research on Internet addiction. *Educational Psychology Review, 17*(4), 363–388.

Chua, C. E. H., Wareham, J., & Robey, D. (2007). The role of online trading communities in managing Internet auction fraud. *MIS Quarterly*, *31*(4), 759-781.

Cohen-Almagor, R. (2013). Online child sex offenders: Challenges and counter-measures. *Howard Journal of Criminal Justice, 52*(2), 190–215.

Copes, H., & Maruna, S. (2017). Techniques of neutralization: A theory of its time and ahead of its time. In T. G. Blomberg, F. T. Cullen, C. Carlsson, & C. Lero

Jonson (Eds.), *Delinquency and drift revisited: The criminology of David Matza and beyond* (Vol. 21, pp. 43–58). New York: Routledge.
Craven S., Brown, S., & Gilchrist, E. (2006). Sexual grooming of children: Review of literature and theoretical considerations. *Journal of Sexual Aggression*, *12*(3), 287–299.
Crone, E. A., & Steinbeis, N. (2017). Neural perspectives on cognitive control development during childhood and adolescence. *Trends in Cognitive Sciences, 21*(3), 205–215.
Davidson, J. C., & Martellozzo, E. (2008). Protecting vulnerable young people in cyberspace from sexual abuse: Raising awareness and responding globally. *Police Practice and Research: An International Journal, 9*(4), 277–289.
Davidson, J., & Bifulco, A. (2018). *Child abuse and protection: Contemporary issues in research, policy and practice*. New York: Routledge.
Davidson, J., & Gottschalk, P. (2011). Characteristics of the Internet for criminal child sexual abuse by online groomers. *Criminal Justice Studies, 24*(1), 23–36.
DeLong, R., Durkin, K., & Hundersmarck, S. (2010). An exploratory analysis of the cognitive distortions of a sample of men arrested in Internet sex stings. *Journal of Sexual Aggression, 16*(1), 59–70.
DeMause, L. (1997). The history of child abuse. *The Journal of Psychohistory, 25*(3), 216–236.
Denyer, D., & Tranfield, D. (2006). Using qualitative research synthesis to build an actionable knowledge base. *Management Decision, 44*(2), 213–227.
Dietz, P. (2018). Grooming and seduction. *Journal of Interpersonal Violence, 33*(1), 28–36.
Dorman Ilan, S., Tamuz, N., & Sheppes, G. (2018). The fit between emotion regulation choice and individual resources is associated with adaptive functioning among young children. *Cognition and Emotion, 33*(3), 597-605.
Duan, W., Gu, B., & Whinston, A. B. (2008). Do online reviews matter?—An empirical investigation of panel data. *Decision Support Systems, 45*(4), 1007–1016.
Durkin, K. F. (2009). There must be some type of misunderstanding, there must be some kind of mistake: The deviance disavowal strategies of men arrested in Internet sex stings (2008 presidential address). *Sociological Spectrum, 29*(6), 661–676.
Durkin, K., & Bryant C. (1999). Propagandizing pederasty: A thematic analysis of the on-line exculpatory accounts of unrepentant pedophiles. *Deviant Behavior, 20*(2), 103–127.
ECPAT. (2016). Terminology guidelines for the protection of children from sexual exploitation and sexual abuse. Terminology and Semantics Interagency Working Group on Sexual Exploitation of Children. Bankok: ECPAT International.
Elliott, I. A. (2016). Applying sexual offence theory to online sex offenders. In D. P. Boer (Ed.), *The wiley handbook on the theories, assessment and treatment of sexual offending*. doi:10.1002/9781118574003.wattso025

Elliott, I. A., Beech, A. R., Mandeville-Norden, R., & Hayes, E. (2009). Psychological profiles of Internet sexual offenders: Comparisons with contact sexual offenders. *Sexual Abuse, 21*(1), 76–92.

Elo, S., & Kyngäs, H. (2008). The qualitative content analysis process. *Journal of Advanced Nursing, 62*(1), 107–115.

Epstein, J. M. (2006). *Generative social science: Studies in agent-based computational modeling*. New Jersey: Princeton University Press.

Epstein, J. M. (2008). Why model? *Journal of Artificial Societies and Social Simulation, 11*(4), 12.

Epstein, J. M., & Axtell, R. (1996). *Growing artificial societies: Social science from the bottom up*. Washington, DC: Brookings Institution Press.

Finkelhor, D., & Dzuiba-Leatherman, J. (1994). Victimization of children. *American Psychologist,* 49(3), 173-183.

Fiske, S. T., & Neuberg, S. L. (1990). A continuum of impression formation, from category-based to individuating processes: Influences of information and motivation on attention and interpretation. In *Advances in experimental social psychology* (Vol. 23, pp. 1–74). San Diego, CA: Academic Press.

Fiske, S. T., & Taylor, S. E. (2017). *Social cognition: From brains to culture* (3rd ed.). Thousand Oaks, CA: Sage.

Fortune, C. A., Bourke, P., & Ward, T. (2015). Expertise and child sex offenders. *Aggression and Violent Behavior, 20*, 33–41.

Fox, J., Cruz, C., & Lee, J. Y. (2015). Perpetuating online sexism offline: Anonymity, interactivity, and the effects of sexist hashtags on social media. *Computers in Human Behavior*, *52*, 436-442.

Gibson, J. J. (1977). The theory of affordances. In R. Shaw & J. Bransford (Eds.), *Perceiving, acting and knowing: Toward an ecological psychology* (pp. 67–88). Hilldale, NJ: Erlbaum.

Gibson, W. (1986). *Neuromancer*. London: Grafton Books.

Gilbert, D. T., Pelham, B. W., & Krull, D. S. (1988). On cognitive busyness: When person perceivers meet persons perceived. *Journal of Personality and Social Psychology, 54*(5), 733-740.

Grabosky, P. N. (2001). Virtual criminality: Old wine in new bottles? *Social & Legal Studies, 10*(2), 243–249.

Grazioli, S. (2004). Where did they go wrong? An analysis of the failure of knowledgeable Internet consumers to detect deception over the Internet. *Group Decision and Negotiation, 13*(2), 149–172.

Grazioli, S., & Järvenpää, S. L. (2000). Perils of Internet fraud: An empirical investigation of deception and trust with experienced Internet consumers. *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans, 30*(4), 395–410.

Grazioli, S., & Järvenpää, S. L. (2003). Consumer and business deception on the Internet: Content analysis of documentary evidence. *International Journal of Electronic Commerce,* 7(4), 93–118.

Greenfield, S. (2015). *Mind change: How digital technologies are leaving their mark on our brains*. New York: Random House Incorporated.

Groff, E. R., Johnson, S. D., & Thornton, A. (2019). State of the art in agent-based modeling of urban crime: An overview. *Journal of Quantitative Criminology, 35*(1), 155–193.

Groff, E. R., Weisburd, D., & Yang, S. M. (2010). Is it important to examine crime trends at a local "micro" level? A longitudinal analysis of street to street variability in crime trajectories. *Journal of Quantitative Criminology, 26*(1), 7–32.

Gupta, A., Kumaraguru, P., & Sureka, A. (2012). Characterizing pedophile conversations on the Internet using online grooming. Retrieved from https://arxiv.org/pdf/1208.4324.pdf

Gutzwiller, R. S., Hunt, S. M., & Lange, D. S. (2016). A task analysis toward characterizing cyber-cognitive situation awareness (CCSA) in cyber defense analysts. In *Cognitive Methods in Situation Awareness and Decision Support (CogSIMA), 2016 IEEE International Multi-Disciplinary Conference on* (pp. 14–20). Piscataway, NJ: IEEE.

Hancock, J. T. (2007). Digital deception. Oxford handbook of internet psychology, 289-301.

Hannah, H. (2017, February 6). Internet safety: A mother's story of how a paedophile groomed her 11-year-old daughter online. *Independent*. Retrieved from https://www.independent.co.uk/life-style/health-and-families/internet-safety-day-hannah-h-mother-paedophile-online-grooming-11-year-old-daughter-facebook-webcam-a7560801.html

Hanson, R. K. (2009). The psychological assessment of risk for crime and violence. *Canadian Psychology/Psychologie Canadienne, 50*(3), 172-182.

Hawi, N. S. (2012). Internet addiction among adolescents in Lebanon. *Computers in Human Behavior, 28*(3), 1044–1053.

Hillman, H., Hooper, C., & Choo, K. K. R. (2014). Online child exploitation: Challenges and future research directions. *Computer Law & Security Review, 30*(6), 687–698.

Hitt, L. M. (1999). Information technology and firm boundaries: Evidence from panel data. *Information Systems Research, 10*(2), 134–149.

Ho, S. M., & Hollister, J. M. (2013, November). Guess who?: an empirical study of gender deception and detection in computer-mediated communication. In *Proceedings of the 76th ASIS&T Annual Meeting: Beyond the Cloud: Rethinking Information Boundaries* (p. 117). American Society for Information Science.

Holt, T. J., Blevins, K. R., & Burkert, N. (2010). Considering the pedophile subculture online. *Sexual Abuse: A Journal of Research and Treatment, 22*(1), 3–24.

Howitt, D., & Sheldon, K. (2007). The role of cognitive distortions in paedophilic offending: Internet and contact offenders compared. *Psychology, Crime & Law, 13(*October), 469–486. http://www.crds.be/userfiles/files/European%20Online%20Grooming%20Project_Final%20Version_140312.pdf

http://www.missingkids.org/content/dam/pdfs/ncmecanalysis/Online%20Enticement%20Pre-Travel.pdf
https://www.unodc.org/documents/commissions/CCPCJ/CCPCJ_Sessions/CCPCJ_23/E-CN15-2014-CRP1_E.pdf

Hui, D. T. L., Xin, C. W., & Khader, M. (2015). Understanding the behavioral aspects of cyber sexual grooming: Implications for law enforcement. *International Journal of Police Science & Management, 17*(1), 40–49.

Hundersmarck, S. F., Durkin, K. F., & Delong, R. L. (2007). Designing a classification system for Internet offenders: Doing cognitive distortions. *Journal of Offender Rehabilitation, 45*(1-2), 257–273.

IOCTA. (2018). *Internet organised crime threat assessment*. Retrieved from https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018

Ivory, A. H., Fox, J., Waddell, T. F., & Ivory, J. D. (2014). Sex role stereotyping is hard to kill: A field experiment measuring social responses to user characteristics and behavior in an online multiplayer first-person shooter game. *Computers in Human Behavior, 35*, 148–156.

IWF. (2016). *IWF Annual Report 2016*. Retrieved from https://www.iwf.org.uk/sites/default/files/reports/2017-04/iwf_report_2016.pdf

IWF. (2017). *Report. Internet Watch Foundation*. Retrieved from https://annualreport.iwf.org.uk/#IWF_the_global_experts

IWF. (2018). *Trends in online child sexual exploitation: Examining the distribution of captures of live-streamed child sexual abuse*. Refrieved from https://www.iwf.org.uk/sites/default/files/inline-files/Distribution%20of%20Captures%20of%20Live-streamed%20Child%20Sexual%20Abuse%20FINAL.pdf

Jaishankar K., (2008). Space Transition Theory of Cyber Crimes. In Schmallager, F., & Pittaro, M. (Eds.), Crimes of the Internet (pp.283-301). Upper Saddle River, NJ: Prentice Hall.

Johnson, G. (2010). Internet use and child development: The techno-microsystem. *Australian Journal of Educational and Developmental Psychology* (AJEDP), *10*, 32–43.

Kahneman, D. (2003). Maps of bounded rationality: A perspective on intuitive judgment and choice. In T. Frangsmyr (Ed.), *Les Prix Nobel: The Nobel Prizes 2002* (pp. 449–489). Stockholm: Nobel Fund.

Kellerman, A. (2014). *The Internet as second action space*. New York: Routledge.

Kellerman, A. (2016). *Geographic interpretations of the Internet*. Switzerland: Springer.

Kerstens, J., & Stol, W. (2014). Receiving online sexual requests and producing online sexual images: The multifaceted and dialogic nature of adolescents' online sexual interactions. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 8*(1).

Keum, B. T., & Miller, M. J. (2018). Racism on the Internet: Conceptualization and recommendations for research. *Psychology of Violence, 8*(6), 782-791.

Kloess, J. A., Beech, A. R., & Harkins, L. (2014). Online child sexual exploitation: Prevalence, process, and offender characteristics. *Trauma, Violence, & Abuse, 15*(2), 126–139.

Kloess, J. A., Seymour-Smith, S., Hamilton-Giachritsis, C. E., Long, M. L., Shipley, D., & Beech, A. R. (2015). A qualitative analysis of offenders' modus operandi in sexually exploitative interactions with children online. *Sexual Abuse: A Journal of Research and Treatment,* 1–29. doi:1177/1079063215612442

Kumar, S. (2005). *Research methodology: A step by step guide for beginners* (2nd ed.). London & Thousand Oaks, CA: Sage.

Lanning, K. (2018). The evolution of grooming: Concept and term. *Journal of Interpersonal Violence, 33*(1), 5–16.

Lapidot-Lefler, N., & Barak, A. (2012). Effects of anonymity, invisibility, and lack of eye-contact on toxic online disinhibition. *Computers in Human Behavior*, *28*(2), 434-443.

Leander, L., Christianson, S. Å., & Granhag, P. A. (2008). Internet ‐ initiated sexual abuse: Adolescent victims' reports about on ‐ and off ‐ line sexual activities. *Applied Cognitive Psychology, 22*(9), 1260–1274.

Lee, A. S. (2001). Editorial. *MIS Quarterly, 25*(1), iii–vii

Lee, J. K. (2015). Research framework for AIS grand vision of the bright ICT initiative. *MIS Quarterly, 39*(2), III–XII.

Leonardi, P. M. (2013). When does technology use enable network change in organizations? A comparative study of feature use and shared affordances. *MIS Quarterly,* 749–775.

Lynd-Stevenson, R. M. (2007). Concerns regarding the traditional paradigm for causal research: The unified paradigm and causal research in scientific psychology. *Review of General Psychology, 11*(3), 286-304.

Mahmood, A., Siponen, M., Straub, D., Rao, R., & Raghu, S. (2010). Moving toward black hat research in information systems security: An editorial introduction to the special issue. *MIS Quarterly, 34*(3), 431–433.

Majchrzak, A., & Markus, M. L. (2012). Technology affordances and constraints in management information systems (MIS). In E., Kessler (Ed.), *Encyclopedia of management theory,* Thousand Oaks, CA: Sage Publications.

Malesky, Jr., L. A., & Ennis, L. (2004). Supportive distortions: An analysis of posts on a pedophile Internet message board. *Journal of Addictions & Offender Counseling, 24*(2), 92–100.

Mann, I. (2017). *Hacking the human: Social engineering techniques and security countermeasures*. New York: Routledge.

Marcum, C. D. (2007). Interpreting the intentions of Internet predators: An examination of online predatory behavior. *Journal of Child Sexual Abuse*, *16*(4), 99-114.

Marcum, C. D., Higgins, G. E., & Ricketts, M. L. (2010). Potential factors of online victimization of youth: An examination of adolescent online behaviors utilizing routine activity theory. *Deviant Behavior, 31*(5), 381–410.

Marcum, C. D., Ricketts, M. L., & Higgins, G. E. (2010). Assessing sex experiences of online victimization: An examination of adolescent online behaviors using routine activity theory. *Criminal Justice Review, 1*, 1–26.

Markus, M. L., & Silver, M. S. (2008). A foundation for the study of IT effects: A new look at DeSanctis and Poole's concepts of structural features and spirit. *Journal of the Association for Information Systems, 9*(10), 609-632.

McCarthy, J. A. (2010). Internet sexual activity: A comparison between contact and non-contact child pornography offenders. *Journal of Sexual Aggression, 16*(2), 181–195.

McGhee, I., Bayzick, J., Kontostathis, A., Edwards, L., McBride, A., & Jakubowski, E. (2011). Learning to identify Internet sexual predation. *International Journal of Electronic Commerce, 15*(3), 103–122.

McManus, M. A., Almond, L., Cubbon, B., Boulton, L., & Mears, I. (2016). Exploring the online communicative themes of child sex offenders. *Journal of Investigative Psychology and Offender Profiling, 13*(2), 166–179.

Miah, W. R., Yearwood, J., & Kulkarni, S. (2014). Constructing an inter-post similarity measure to differentiate the psychological stages in offensive Chats. *Journal of the Association for Information Science and Technology, 66*(5), 1065–1081.

Michalopoulos, D., Mavridis, I., & Jankovic, M. (2014). ScienceDirect GARS : Real-time system for identification, assessment and control of cyber grooming attacks. *Computers & Security, 42*, 177–190.

Middleton, D., Elliott, I. A., Mandeville-Norden, R., & Beech, A. R. (2006). An investigation into the applicability of the Ward and Siegert pathways model of child sexual abuse with Internet offenders. *Psychology, Crime & Law, 12*(6), 589–603

Mitchell, K. J., Wolak, J., & Finkelhor, D. (2007). Trends in youth reports of sexual solicitations, harassment and unwanted exposure to pornography on the *Internet. Journal of Adolescent Health*, 40(2), 116-126.

Moore, M. J., Nakano, T., Enomoto, A., & Suda, T. (2012). Anonymity and roles associated with aggressive posts in an online forum. *Computers in Human Behavior, 28*(3), 861–867.

Munzert, S., Rubba, C., Meißner, P., & Nyhuis, D. (2014). *Automated data collection with R: A practical guide to web scraping and text mining*. Chicester, UK: John Wiley & Sons.

Murumaa-Mengel, M. (2015). Drawing the threat: A study on perceptions of the online pervert among Estonian high school students. *Young, 23*(1), 1–18.

Navarro, J. N., & Jasinski, J. L. (2015). Demographic and motivation differences among online sex offenders by type of offense: An exploration of routine activities theories. *Journal of Child Sexual Abuse, 24*(7), 753–771.

NCMEC. (2017). The online enticement of children: An in-depth analysis of cybertipline reports. Retrieved from

NSPCC. (2018a). Preventing abuse, child abuse and neglect Retrieved from https://www.nspcc.org.uk/preventing-abuse/child-abuse-and-neglect/child-sexual-abuse/

NSPCC. (2018b). Over 3,000 new grooming offences recorded since last year. Retrieved from https://bit.ly/2kX7TuD

O'Connell, R. (2003). *A typology of child cybersexploitation and online grooming practices*. Preston, UK: University of Central Lancashire.

Okoli, C., & Schabram, K. (2010). A guide to conducting a systematic literature review of information systems research. *Sprouts: Working Papers on Information Systems, 10*(26). Retrieved from http://sprouts.aisnet.org/10-26

Olafson, E., Corwin, D. L., & Summit, R. C. (1993). Modern history of child sexual abuse awareness: Cycles of discovery and suppression. *Child Abuse & Neglect, 17*(1), 7–24.

Olson, L. N., Daggs, J. L., Ellevold, B. L., & Rogers, T. K. (2007). Entrapping the innocent: Toward a theory of child sexual predators' luring communication. *Communication Theory, 17*(3), 231–251.

Orlikowski, W. J. (1989). Division among the ranks: The social implications of CASE tools for system developers. *Proceedings of the Tenth International Conference on Information Systems*, Boston, MA, 1989, pp. 199-210.

Orlikowski, W. J., & Baroudi, J. J. (1991). Studying information technology in organizations: Research approaches and assumptions. *Information Systems Research, 2*(1), 1–28.

Paas, F., Tuovinen, J. E., Tabbers, H., & Van Gerven, P. W. (2003). Cognitive load measurement as a means to advance cognitive load theory. *Educational Psychologist*, *38*(1), 63–71.

Palasinski, M. (2012). The roles of monitoring and cyberbystanders in reducing sexual abuse. *Computers in Human Behavior, 28*(6), 2014–2022.

Papaioannou, D., Sutton, A., Carroll, C., Booth, A., & Wong, R. (2010). Literature searching for social science systematic reviews: Consideration of a range of search techniques. *Health Information & Libraries Journal, 27*(2), 114–122.

Paré, G., Trudel, M. C., Jaana, M., & Kitsiou, S. (2015). Synthesizing information systems knowledge: A typology of literature reviews. *Information & Management, 52*(2), 183–199.

Poli, R. (2017). Internet addiction update: Diagnostic criteria, assessment and prevalence. *Neuropsychiatry, 7*(1), 04–08.

Pozzi, G., Pigni, F., & Vitari, C. (2014). Affordance theory in the IS discipline: A review and synthesis of the literature. *Proceedings of the 20th Americas Conference on Information Systems (AMCIS 2014): Smart Sustainability: The Information Systems Opportunity* (Vol. 4, pp. 3809–3820). New York: Curran Associates.

Pranoto, H., Gunawan, F. E., & Soewito, B. (2015). Logistic models for classifying online grooming conversation. *Procedia Computer Science, 59*, 357–365.

Pratt, T. C. (2017). Delinquency and drift: Challenging criminology then and now. In T. G. Blomberg, F. T. Cullen, C. Carlsson, & C. Lero Jonson (Eds.), *Delinquency and Drift Revisited: The criminology of David Matza and beyond* (Vol. 21, pp. 13–30). New York: Routledge.

Pratt, T. C., Holtfreter, K., & Reisig, M. D. (2010). Routine online activity and Internet fraud targeting: Extending the generality of routine activity theory. *Journal of Research in Crime and Delinquency, 47*(3), 267–296.

Quayle, E., & Newman, E. (2015). The role of sexual images in online and offline sexual behaviour with minors. *Current Psychiatry Reports,* 17(6), 1-6.

Quayle, E., & Taylor, M. (2003). Model of problematic Internet use in people with a sexual interest in children. *Cyber Psychology & Behavior, 6*(1), 93–106.

Quayle, E., Allegro, L., & Hutton, L. (2012). *Online behaviour related to child sexual abuse: Creating a private space in which to offend. Interviews with online child sex offenders*. Copenhagen: Council of the Baltic Sea States.

Quayle, E., Allegro, S., Hutton, L., Sheath, M., & Lööf, L. (2014). Rapid skill acquisition and online sexual grooming of children. *Computers in Human Behavior, 39*, 368–375.

Quayle, E., Holland, G., Linehan, C., & Taylor, M. (2000). The Internet and offending behaviour: A case study. *Journal of Sexual Aggression*, 6(1-2), 78–96.

Radbill, S. X. (1968). *A history of child abuse and infanticide*. Chicago: University of Chicago Press.

Radford, L., Corral, S., Bradley, C., Fisher, H., Bassett, C., Howat, N., & Collishaw, S. (2011). *Child abuse and neglect in the UK today*. Retrieved from https://learning.nspcc.org.uk/media/1042/child-abuse-neglect-uk-today-research-report.pdf

Ronkin, M., & Karn, H. E. (1999). Mock ebonics: Linguistic racism in parodies of ebonics on the Internet. *Journal of Sociolinguistics, 3*(3), 360–380.

Sarker, S., Xiao, X., & Beaulieu, T. (2013). Guest editorial: Qualitative studies in information systems: a critical review and some guiding principles. *MIS Quarterly, 37*(4), iii–xviii.

Schachar, R., & Logan, G. D. (1990). Impulsivity and inhibitory control in normal development and childhood psychopathology. *Developmental Psychology, 26*(5), 710-720.

Schouten, A. P., Valkenburg, P. M., & Peter, J. (2007). Precursors and underlying processes of adolescents' online self-disclosure: Developing and testing an "Internet-attribute-perception" model. *Media Psychology, 10*(2), 292–315.

Schreier, M. (2014). Qualitative content analysis. *SAGE handbook of qualitative data analysis* (pp. 170–183). London: Sage.

Schwarzer, R. (2008). Modeling health behavior change: How to predict and modify the adoption and maintenance of health behaviors. *Applied Psychology, 57*(1), 1–29.

Seidel, S., Recker, J., & Vom Brocke, J. (2013). Sensemaking and sustainable practicing: Functional affordances of information systems in green transformations. *MIS Quarterly,* 37(4), 1275–1299.

Shapira, N. A., Goldsmith, T. D., Keck Jr., P. E., Khosla, U. M., & McElroy, S. L. (2000). Psychiatric features of individuals with problematic Internet use. *Journal of Affective Disorders, 57*(1-3), 267–272.

Steinfeldt, J. A., Foltz, B. D., Kaladow, J. K., Carlson, T. N., Pagano Jr., L. A., Benton, E., & Steinfeldt, M. C. (2010). Racism in the electronic age: Role of online forums in expressing racial attitudes about American Indians. *Cultural Diversity and Ethnic Minority Psychology, 16*(3), 1-9.

Stewart, J., & Dawson, M. (2018). How the modification of personality traits leave one vulnerable to manipulation in social engineering. *International Journal of Information Privacy, Security and Integrity, 3*(3), 187–208.

Suler J. (2004). The online disinhibition effect. *CyberPsychology & Behavior, 7*(3), 321–326

Surjadi, B., Bullens, R., van Horn, J., & Bogaerts, S. (2010). Internet offending: Sexual and non-sexual functions within a Dutch sample. *Journal of Sexual Aggression, 16*(1), 47–58.

Sweller, J. (2011). Cognitive load theory. In *Psychology of learning and motivation: Cognition in education* (Vol. 55, pp. 37–76). San Diego, CA: Academic Press.

Topalli, V., & O'Neal, E. C. (2003). Retaliatory motivation enhances attributions of hostility when people process ambiguous social stimuli. *Aggressive Behavior: Official Journal of the International Society for Research on Aggression, 29*(2), 155–172.

Topalli, V., & Wright, R. (2013). Affect and the dynamic foreground of predatory street crime: Desperation, anger and fear. In J.-L. van Gelder, H. Elffers, D. Reynald, & D. Nagin (Eds.), *Affect and cognition in criminal decision making* (pp. 60–75). New York: Routledge.

Treuer, T., Fábián, Z., & Füredi, J. (2001). Internet addiction associated with features of impulse control disorder: Is it a real psychiatric disorder? *Journal of Affective Disorders–66*(2-3), 283.

Tsikerdekis, M., & Zeadally, S. (2014). Online deception in social media. *Communications of the ACM*, 57(9), 72.

UNODC. (2014). *Study facilitating the identification, description and evaluation of the effects of new information technologies on the abuse and exploitation of children*. Retrieved from

Vale, J. R., & Vale, C. A. (1969). Individual differences and general laws in psychology: A reconciliation. *American Psychologist, 24*(12), 1093-1180.

Van der Hof, S., & Koops, B. J. (2011). Adolescents and cybercrime: Navigating between freedom and control. *Policy & Internet, 3*(2), 1–28.

Vartapetiance, A., & Gillam, L. (2014). "Our Little Secret": Pinpointing potential predators. *Security Informatics, 3*(3), 1–19.

Velicer, W. F., & Prochaska, J. O. (2008). Stage and non-stage theories of behavior and behavior change: A comment on schwarzer. *Applied Psychology, 57*(1), 75–83.

Venkatesh, V., Brown, S. A., & Bala, H. (2013). Bridging the qualitative-quantitative divide: Guidelines for conducting mixed methods research in information systems. *MIS Quarterly,* 21–54.

Volkoff, O., & Strong, D. M. (2013). Critical realism and affordances: Theorizing IT-associated organizational change processes. *MIS Quarterly,* 37(3), 819–834.

Wachs, S., Whittle, H. C., Hamilton-Giachritsis, C., Wolf, K. D., Vazsonyi, A. T., & Junger, M. (2018). Correlates of mono-and dual-victims of cybergrooming and cyberbullying: Evidence from four countries. *CyberPsychology, Behavior, and Social Networking, 21*(2), 91–98.

Wall, G. K., Pearce, E., & Mcguire, J. (2011). Are Internet offenders emotionally avoidant ? *Psychology, Crime & Law, 17*(5), 381–401.

Wallace, P. (2015). *The psychology of the Internet*. Cambridge: Cambridge University Press.

Walsham, G. (1995). Interpretive case studies in IS research: Nature and method. *European Journal of Information Systems, 4*(2), 74–81.

Walsham, G. (2006). Doing interpretive research. *European Journal of Information Systems, 15*(3), 320–330.

Wang, Y., Meister, D. B., & Gray, P. H. (2013). Social influence and knowledge management systems use: Evidence from panel data. *MIS Quarterly,* 37(1), 299–313.

Webster, J., & Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. *MIS Quarterly,* 26(2), xiii–xxiii.

Webster, S., & Davidson, J., Bifulco, A., Gottschalk, P., Caretti, V., Pham, T., … Craparo, G. (2012). *European Online Grooming Project – Final report*. Retrieved from

Weinstein, N. D., Rothman, A. J., & Sutton, S. R. (1998). Stage theories of health behavior: Conceptual and methodological issues. *Health Psychology,* 17(3), 290-299.

Wells, M., & Mitchell, K. J. (2014). Patterns of Internet use and risk of online victimization for youth with and without disabilities. *Journal of Special Educcation, 48*(3), 204–213.

Wells, M., & Mitchelln K. J. (2008). How do high-risk youth use the Internet? Characteristics and implications for prevention. *Child Maltreatment, 13*(3), 227–234.

Whittle, H., Hamilton-Giachritsis, C., & Beech, A. (2014). "Under His Spell": Victims' perspectives of being groomed online. *Social Sciences, 3*(3), 404–426.

Whittle, H., Hamilton-Giachritsis, C., Beech, A., & Collings, G. (2013). Aggression and violent behavior a review of online grooming: Characteristics and concerns. *Aggression and Violent Behavior, 18*(1), 62–70.

WHO. (2003). *Guidelines for medico-legal care for victims of sexual violence*. Geneva: World Health Organization.

Williams, R., Elliott, I. A., & Beech, A. R. (2013). identifying sexual grooming themes used by Internet sex offenders Internet sex offenders. *Deviant Behavior, 34*(2), 135–152.

Winder, B., Gough, B., & Seymour-Smith, S. (2015). Stumbling into sexual crime: The passive perpetrator in accounts by male Internet sex offenders. *Archives of Sexual Behavior, 44*(1), 167–180.

Wolak, J., Finkelhor, D., & Mitchell, K. J. (2009). Trends in arrests of "online predators." Retrieved from http://unh.edu/ccrc/pdf/N-JOV2_methodology_report.pdf

Wotela, K. (2017). Conceptualising conceptual frameworks in public and business management research. *Proceedings of European Conference on Research Methodology for Business and Management Studies* (pp. 370–379). Oxford: Academic Conferences International Limited.

Wurtele, S. K., & Kenny, M. C. (2016). Technology-related sexual solicitation of adolescents: A review of prevention efforts. *Child Abuse Review, 25*(5), 332–344.

Xiao, B., & Benbasat, I. (2011). Product-related deception in e-commerce: a theoretical perspective. Mis Quarterly, 35(1), 169-196.

Yellowlees, P. M., & Marks, S. (2007). Problematic Internet use or Internet addiction?. *Computers in Human Behavior*, *23*(3), 1447–1453.

Yoo, Y. (2010). Computing in everyday life: A call for research on experiential computing. *MIS Quarterly,* 34(2), 213–231.

Yoo, Y., Boland Jr., R. J., Lyytinen, K., & Majchrzak, A. (2012). Organizing for innovation in the digitized world. *Organization Science*, *23*(5), 1398–1408.

Young, K. S. (1998). Internet addiction: The emergence of a new clinical disorder. *Cyberpsychology & Behavior, 1*(3), 237–244.

Zachariadis, M., Scott, S. V., & Barrett, M. I. (2010). Designing mixed-method research inspired by a critical realism philosophy: A tale from the field of IS innovation. In *ICIS 2010 Proceedings* (p. 265).

Zammuto, R. F., Griffith, T. L., Majchrzak, A., Dougherty, D. J., & Faraj, S. (2007). Information technology and the changing fabric of organization. *Organization Science*, *18*(5), 749–762. Retrieved from https://aisel.aisnet.org/icis2010_submissions/265

Zimmerman, A. G., & Ybarra, G. J. (2016). Online aggression: The influences of anonymity and social modeling. *Psychology of Popular Media Culture*, *5*(2), 1-44.

APPENDICES

APPENDIX 1 Included papers in SLRA (omitted)

Included and coded papers												
Included papers	Atheoretical (AT)	Atheoretical with	Theoretical	Theory Building	Empirical	Conceptual	Offender	Victim	Motivation	Act	Internet	Other
1. Agustina, J. R. (2015). Understanding Cyber Victimization : Digital Architectures and the Disinhibition Effect. International Journal of Cyber Criminology (IJCC), 9(1), 35–54. https://doi.org/10.5281/zenodo.22239		X				X		X			X	
2. Albert, C. S., & Salam, A. F. (2011). Protecting Children Online: Identifying Registered Sex Offenders Presence On The Internet And Consequent Online Social Behavior. *Thirty Second International Conference on Information Systems, Shanghai*, 1–12.				X		X	X					X
3. Albert, C. S., & Salam, A. F. (2012). Predatory Coercion In Social Media And Protection Of Children Online – A Critical Discourse Analysis Approach. *Thirty Third International Conference on Information Systems, Orlando 2012*.				X	X		X			X		

Included and coded papers												
Included papers	Atheoretical (AT)	Atheoretical with	Theoretical	Theory Building	Empirical	Conceptual	Offender	Victim	Motivation	Act	Internet	Other
4. Ashurst, L., & Mcalinden, A. (2015). Young people , peer-to-peer grooming and sexual offending : Understanding and responding to harmful sexual behaviour within a social media society. *Probation Journal*, *62*(4), 374–388. https://doi.org/10.1177/0264550515619572	X					X	X					X
5. Aslan, D. (2010). Critically Evaluating Typologies of Internet Sex Offenders : A Psychological Perspective. *Journal of Forensic Psychology Practice, 11*, 406–431. https://doi.org/10.1080/15228932.2011.588925	X				X		X		X			
6. Aslan, D. & Edelmann, R. (2014). Demographic and offence characteristics : a comparison of sex offenders convicted of possessing indecent images of children , committing contact sex offences or both offences. *The Journal of Forensic Psychiatry & Psychology*, *25*(2), 121–134. https://doi.org/10.1080/14789949.2014.884618	X					X	X		X			
7. 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*(1), 45–66. https://doi.org/10.1007/s10508-014-0270-x		X			X		X		X			
8. Babchishin, K. M., Hanson, R. K., & Hermann, C. A. (2011). The characteristics of online sex offenders: A meta-analysis. *Sexual Abuse a Journal of Research and Treatment*, *23*(1), 92–123. https://doi.org/10.1177/1079063210370708		X			X		X		X			

Included and coded papers												
Included papers	Atheoretical (AT)	Atheoretical with	Theoretical	Theory Building	Empirical	Conceptual	Offender	Victim	Motivation	Act	Internet	Other
9. 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.	X					X	X				X	
10. Barber, C. S., & Bettez, S. C. (2014). Deconstructing the online grooming of youth: Toward improved information systems for detection of online sexual predators. *Thirty Fifth International Conference on Information Systems, Auckland 2014*, 1–20. Retrieved from http://www.scopus.com/inward/record.url?eid=2-s2.0-84923395579&partnerID=tZOtx3y1				X	X		X	X		X		
11. Bates, A., & Metcalf, C. (2007). A psychometric comparison of internet and non-internet sex offenders from a community treatment sample. *Journal of Sexual Aggression*, *13*(1), 11–20. https://doi.org/10.1080/13552600701365654	X				X		X		X			
12. 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*(3), 216–228. https://doi.org/10.1016/j.avb.2008.03.007	X					X	X					X
13. Bergen, E., Ahto, A., Schulz, A., Imhoff, R., Antfolk, J., Schuhmann, P., … Jern, P. (2015). Adult-Adult and Adult-Child/Adolescent Online Sexual Interactions: An Exploratory Self-Report Study on the Role of Situational Factors. *Journal of Sex Research*, *52*(9), 1006–1016. https://doi.org/10.1080/00224499.2014.914462	X				X		X		X			

Included and coded papers												
Included papers	Atheoretical (AT)	Atheoretical with	Theoretical	Theory Building	Empirical	Conceptual	Offender	Victim	Motivation	Act	Internet	Other
14. Berson, M. J., & Berson, I. R. (2003). Lessons Learned About Schools and Their Responsibility to Foster Safety Online. *Journal of School Violence*, *2*(1), 105–117. https://doi.org/10.1300/J202v02n01	X					X		X				X
15. Black, P. J., Wollis, M., Woodworth, M., & Hancock, J. T. (2014). A linguistic analysis of grooming strategies of online child sex offenders: Implications for our understanding of predatory sexual behavior in an increasingly computer-mediated world. *Child Abuse and Neglect*, *44*, 140–149. https://doi.org/10.1016/j.chiabu.2014.12.004			X		X		X			X		
16. Briggs, P., Simon, W. T., & Simonsen, S. (2011). An exploratory study of Internet-initiated sexual offenses and the chat room sex offender: has the Internet enabled a new typology of sex offender? *Sexual Abuse : A Journal of Research and Treatment*, *23*(1), 72–91.	X				X		X		X			
17. Buschman, J., Bogaerts, S., Foulger, S., Wilcox, D., Sosnowski, D., & Cushman, B. (2009). Sexual History Disclosure Polygraph Examinations With Cybercrime Offences: A First Dutch Explorative Study. *International Journal of Offender Therapy and Comparative Criminology*, *54*(3), 395–411. https://doi.org/10.1177/0306624X09334942	X				X		X					X
18. Buschman, J., Wilcox, D., Krapohl, D., Oelrich, M., & Hackett, S. (2010). Cybersex offender risk assessment. An explorative study. *Journal of Sexual Aggression*, *16*(August 2015), 197–209. https://doi.org/10.1080/13552601003690518	X				X		X		X			

Included and coded papers												
Included papers	Atheoretical (AT)	Atheoretical with	Theoretical	Theory Building	Empirical	Conceptual	Offender	Victim	Motivation	Act	Internet	Other
19. Cano, A. E., Fernandez, M., & Alani, H. (2014). Social Informatics 6th International Conference, SocInfo 2014 Barcelona, Spain, November 11-13, 2014 Proceedings 13. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *8851*(November 2016). https://doi.org/10.1007/978-3-319-13734-6		X			X		X	X		X		
20. Chawki, M. 2009. (2008). Online Child Sexual Abuse: The Law Enforcement Response. *Journal of Digital Forensics, Security and Law*, *4*(4), 7–37. https://doi.org/436	X					X	X			X		
21. Cohen-Almagor, R. (2013). Online Child Sex Offenders: Challenges and Counter-Measures. *Howard Journal of Criminal Justice*, *52*(2), 190–215. https://doi.org/10.1111/hojo.12006			X		X		X					X
22. Craven, S., Brown, S., & Gilchrist, E. (2006). Sexual grooming of children: Review of literature and theoretical considerations. *Journal of Sexual Aggression*, *12*(3), 287–299. https://doi.org/10.1080/13552600601069414		X				X	X		X	X		
23. Craven, S., Brown, S., & Gilchrist, E. (2007). Current Responses to Sexual Grooming: Implication for Prevention. *The Howard Journal*, *46*(1), 60–71. https://doi.org/10.1111/j.1468-2311.2007.00454.x	X					X	X					X
24. Davidson, J., & Gottschalk, P. (2011). Characteristics of the Internet for criminal child sexual abuse by online groomers. *Criminal Justice Studies*, *24*(1), 23–36. https://doi.org/10.1080/1478601X.2011.544188		X				X	X				X	

Included and coded papers												
Included papers	Atheoretical (AT)	Atheoretical with	Theoretical	Theory Building	Empirical	Conceptual	Offender	Victim	Motivation	Act	Internet	Other
25. Davidson, J. C., & Martellozzo, E. (2008). Protecting vulnerable young people in cyberspace from sexual abuse: raising awareness and responding globally. *Police Practice and Research*, *9*(4), 277–289. https://doi.org/10.1080/15614260802349965		X			X			X				X
26. Davidson, J. (2007). Current Practice and Research into Internet Sex Offending. *Risk Management*, (January), 89. https://doi.org/262		X			X		X			X		
27. DeLong, R., Durkin, K., & Hundersmarck, S. (2010). An exploratory analysis of the cognitive distortions of a sample of men arrested in internet sex stings. *Journal of Sexual Aggression*, *16*(1), 59–70. https://doi.org/http://dx.doi.org/10.1080/13552600903428235				X	X		X		X			
28. Dombrowski, G. & D. 2007. (2008). How do Child and Family Social Workers Talk to Parents about Child Welfare Concerns ? *Child Abuse Review*, *17*(December 2006), 23–35. https://doi.org/10.1002/car	X					X		X				X
29. Durkin, K., & Bryant, C. (1999). Propagandizing Pederasty: a Thematic Analysis of the on-Line Exculpatory Accounts of Unrepentant Pedophiles. *Deviant Behavior*, *20*(2), 103–127. https://doi.org/10.1080/016396299266524		X			X		X		X			
30. Durkin, K. F. (2009). There Must Be Some Type of Misunderstanding, There Must Be Some Kind of Mistake: The Deviance Disavowal Strategies of Men Arrested in Internet Sex Stings (2008 Presidential Address). *Sociological Spectrum*, *29*(6), 661-676.	X				X		X		X			

Included and coded papers												
Included papers	Atheoretical (AT)	Atheoretical with	Theoretical	Theory Building	Empirical	Conceptual	Offender	Victim	Motivation	Act	Internet	Other
31. Elliott, I. A., & Ashfield, S. (2011). The use of online technology in the modus operandi of female sex offenders. *Journal of Sexual Aggression*, *17*(1), 92–104. https://doi.org/10.1080/13552600.2010.537379	X					X	X			X		
32. Elliott, I. A. (2015). A Self-Regulation Model of Sexual Grooming. *Trauma, Violence, & Abuse*, *18*(1), 83–97. https://doi.org/10.1177/1524838015591573				X		X	X			X		
33. Elliott, I. A., Beech, A. R., Mandeville-Norden, R., & Hayes, E. (2009). Psychological profiles of internet sexual offenders: comparisons with contact sexual offenders. *Sexual Abuse : A Journal of Research and Treatment*, *21*(1), 76–92. https://doi.org/10.1177/1079063208326929		X			X		X		X			
34. Elliott, I. A., Beech, A. R., & Mandeville-Norden, R. (2013). The Psychological Profiles of Internet, Contact, and Mixed Internet/Contact Sex Offenders. *Sexual Abuse: A Journal of Research and Treatment*, *25*(1), 3–20. https://doi.org/10.1177/1079063212439426	X				X		X		X			
35. Eneman, M., Gillespie, A. A., & Bernd, C. S. (2010). Technology and Sexual Abuse: A Critical Review of an Internet Grooming Case. *ICIS 2010 Proceedings*.	X					X	X				X	
36. Frank, R., Westlake, B., & Bouchard, M. (2010). The structure and content of online sexual exploitation networks. *SIGKDD Workshop on Intelligence and Security Informatics*, 1–9.	X				X		X					X

Included and coded papers												
Included papers	Atheoretical (AT)	Atheoretical with	Theoretical	Theory Building	Empirical	Conceptual	Offender	Victim	Motivation	Act	Internet	Other
37. Gallagher, B. (2007). Internet-initiated incitement and conspiracy to commit child sexual abuse (CSA): The typology, extent and nature of known cases. *Journal of Sexual Aggression*, *13*(2), 101–119. https://doi.org/10.1080/13552600701521363	X				X		X			X		
38. Gillespie, A. A. (2004). Tackling grooming. *The Police Journal*, *77*(3), 239-255.	X					X	X			X		X
39. Gillespie, A. A. (2008). Cyber-Stings : Policing Sex Offences on the Internet. *The Police Journal*, *81*, 196–208. https://doi.org/10.1358/pojo.2008.81.3.415	X					X	X			X		
40. Gottschalk, P., & Kristoffersen, R. (2009). Understanding the process of online grooming: The behavior of men who target young people online in Norway. *International Journal of Digital Crime and Forensics*, *1*(4), 1–18. https://doi.org/10.4018/jdcf.2009062401	X					X	X					X
41. Gupta, A., Kumaraguru, P., & Sureka, A. (2012). Characterizing Pedophile Conversations on the Internet using Online Grooming. *arXiv*, *1208.4324v*([cs.CY]), 4324. Retrieved from http://arxiv.org/abs/1208.4324			X		X		X			X		
42. Hillman, H., Hooper, C., & Choo, K. K. R. (2014). Online child exploitation: Challenges and future research directions. *Computer Law and Security Review*, *30*(6), 687–698. https://doi.org/10.1016/j.clsr.2014.09.007		X				X	X					X
43. van der Hof, S., & Koops, B. J. (2011). Adolescents and cybercrime: Navigating between freedom and control. *Policy & Internet*, *3*(2), 1-28.	X					X		X	X			

Included and coded papers												
Included papers	Atheoretical (AT)	Atheoretical with	Theoretical	Theory Building	Empirical	Conceptual	Offender	Victim	Motivation	Act	Internet	Other
44. Holt, T. J., Blevins, K. R., & 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	X				X		X			X		
45. Houtepen, J. A. B. M., Sijtsema, J. J., & Bogaerts, S. (2014). From child pornography offending to child sexual abuse: A review of child pornography offender characteristics and risks for cross-over. *Aggression and Violent Behavior*, *19*(5), 466–473. https://doi.org/10.1016/j.avb.2014.07.011	X					X	X		X			
46. Howitt, D., & Sheldon, K. (2007). The role of cognitive distortions in paedophilic offending: Internet and contact offenders compared. *Psychology, Crime & Law*, *13*(October), 469–486. https://doi.org/10.1080/10683160601060564			X		X		X		X			
47. Hui, D. T. L., Xin, C. W., & Khader, M. (2015). Understanding the behavioral aspects of cyber sexual grooming: Implications for law enforcement. *International Journal of Police Science {&} Management*, *17*(1), 40–49. https://doi.org/10.1177/1461355714566782		X				X	X	X	X	X		X
48. Hundersmarck, D. L. and H. (2007). Designing a Classification System for Internet Offenders. *Journal of Offender Rehabilitation*, *45*(1–2), 149–165. https://doi.org/10.1300/J076v45n01				X		X	X		X			
49. Jewkes, Y., & Wykes, M. (2012). Reconstructing the sexual abuse of children: "cyber-paeds", panic and power. *Sexualities*, *15*(8), 934–952. https://doi.org/10.1177/1363460712459314			X		X		X		X			

Included and coded papers												
Included papers	Atheoretical (AT)	Atheoretical with	Theoretical	Theory Building	Empirical	Conceptual	Offender	Victim	Motivation	Act	Internet	Other
50. Jewkes, Y. (2010). Much ado about nothing? Representations and realities of online soliciting of children. *Journal of Sexual Aggression*, *16*(1), 5–18. https://doi.org/10.1080/13552600903389452	X					X	X	X	X			X
51. Katz, C. (2013). Internet-related child sexual abuse: What children tell us in their testimonies. *Children and Youth Services Review*, *35*(9), 1536–1542. https://doi.org/10.1016/j.childyouth.2013.06.006				X	X			X		X		
52. Kerstens, J., & Stol, W. (2014). Receiving online sexual requests and producing online sexual images: The multifaceted and dialogic nature of adolescents' online sexual interactions. *Cyberpsychology*, *8*(1). https://doi.org/10.5817/CP2014-1-8	X				X			X	X		X	
53. Kierkegaard, S. (2008). Cybering, online grooming and ageplay. *Computer Law and Security Report*, *24*(1), 41–55. https://doi.org/10.1016/j.clsr.2007.11.004	X					X	X					X
54. Kloess, J. A., Beech, A. R., & Harkins, L. (2014). Online Child Sexual Exploitation: Prevalence, Process, and Offender Characteristics. *Trauma, Violence, {&} Abuse*, *15*(2), 126–139. https://doi.org/10.1177/1524838013511543				X		X	X			X	X	
55. Kloess, J. A., Seymour-Smith, S., Hamilton-Giachritsis, C. E., Long, M. L., Shipley, D., & Beech, A. R. (2015). A Qualitative Analysis of Offenders' Modus Operandi in Sexually Exploitative Interactions With Children Online. *Sexual Abuse: A Journal of Research and Treatment*, 1–29. https://doi.org/10.1177/1079063215612442	X				X		X		X	X		

Included and coded papers												
Included papers	Atheoretical (AT)	Atheoretical with	Theoretical	Theory Building	Empirical	Conceptual	Offender	Victim	Motivation	Act	Internet	Other
56. Krueger, R. B., Kaplan, M. S., & First, M. B. (2009). Sexual and other axis I diagnoses of 60 males arrested for crimes against children involving the Internet. *CNS Spectrums*, *14*(June 2016), 623–631.	X				X		X		X			
57. Laulik, S., Allam, J., & Sheridan, L. (2007). An investigation into maladaptive personality functioning in Internet sex offenders. *Psychology, Crime & Law*, *13*(5), 523–535. https://doi.org/10.1080/10683160701340577	X				X		X		X			
58. Leander, L., Christianson, S., & Granhag, P.-A. (2008). Parent – Child Talk and Children ' s Memory for Stressful Events. *Applied Cognitive Psychology*, *21*(December 2006), 1057–1075. https://doi.org/10.1002/acp	X				X			X				X
59. Leonard, M. M. (2010). "I did what I was directed to do but he didn't touch me": The impact of being a victim of internet offending. *Journal of Sexual Aggression*, *16*(2), 249–256. https://doi.org/10.1080/13552601003690526	X					X		X				X
60. Long, M. L., Alison, L. A., & Mcmanus, M. A. (2016). Child Pornography and Likelihood of Contact Abuse: A Comparison Between Contact Child Sexual Offenders and Noncontact Offenders. *Sexual Abuse: A Journal of Research and Treatment*, *XX*, 1–26. https://doi.org/10.1177/1079063212464398	X				X		X		X			
61. Malesky Jr., L. A., & Ennis, L. (2004). Supportive Distortions: An Analysis of Posts on a Pedophile Internet Message Board. *Journal of Addictions & Offender Counseling*, *24*(April), 92–100. https://doi.org/10.1002/j.2161-1874.2004.tb00185.x		X			X		X		X		X	

Included and coded papers												
Included papers	Atheoretical (AT)	Atheoretical with	Theoretical	Theory Building	Empirical	Conceptual	Offender	Victim	Motivation	Act	Internet	Other
62. Malesky Jr, L. A. (2007). Predatory online behavior: Modus operandi of convicted sex offenders in identifying potential victims and contacting minors over the Internet. *Journal of child sexual abuse*, *16*(2), 23-32.	X				X		X			X		
63. Marcum, C. (2007). Interpreting the Intentions of Internet Predators: An Examination of Online Predatory Behavior. *Journal of Child Sexual Abuse*, *16*(4), 99–114. https://doi.org/10.1300/J070v16n04	X				X		X		X			
64. Marcum, C. D., Higgins, G. E., & Ricketts, M. L. (2010). Potential factors of online victimization of youth: An examination of adolescent online behaviors utilizing routine activity theory. *Deviant Behavior*, *31*(5), 381–410. https://doi.org/10.1080/01639620903004903			X		X			X	X			
65. Marcum, C. D., Ricketts, M. L., & Higgins, G. E. (2010). Assessing Sex Experiences of Online Victimization : An Examination of Adolescent Online Behaviors Using Routine Activity Theory. *Criminal Justice Review*, *000(00) 1-*, 1–26. https://doi.org/10.1177/0734016809360331			X		X			X	X			
66. Mccartan, K. F., & Mcalister, R. (2012). Mobile phone technology and sexual abuse. Information & Communications Technology Law, 21:3(October), 257–268. https://doi.org/10.1080/13600834.2012.744223	X					X	X			X	X	

Included and coded papers												
Included papers	Atheoretical (AT)	Atheoretical with	Theoretical	Theory Building	Empirical	Conceptual	Offender	Victim	Motivation	Act	Internet	Other
67. McGhee, I., Bayzick, J., Kontostathis, A., Edwards, L., McBride, A., & Jakubowski, E. (2011). Learning to Identify Internet Sexual Predation. *International Journal of Electronic Commerce*, *15:3*(July), 103–122. https://doi.org/10.2753/JEC1086-4415150305		X			X		X			X		
68. Mcgrath, M. G., & Casey, E. (2002). Forensic Psychiatry and the Internet : Practical Perspectives on Sexual Predators and Obsessional Harassers in Cyberspace. *The Journal of the American Academy of Psychiatry and the Law*, *30*(1), 81–94.	X					X	X				X	
69. Mcmanus, M. A., Almond, L., Cubbon, B. E. N., Boulton, L., & Mears, I. A. N. (2015). Exploring the Online Communicative Themes of Child Sex Offenders. *Journal of Investigative Psychology and Offender Profiling*.		X			X		X			X		
70. Miah, W. R., Yearwood, J., & Kulkarni, S. (2014). Constructing an Inter-Post Similarity Measure to Differentiate the Psychological Stages in Offensive Chats. *Journal of the Association for Information Science and Technology*, *66*(5), 1065–1081. https://doi.org/10.1002/asi		X			X		X	X		X		
71. Michalopoulos, D., Mavridis, I., & Jankovic, M. (2014). ScienceDirect GARS : Real-time system for identification , assessment and control of cyber grooming attacks. *Computers & Security*, *42*, 177–190. https://doi.org/10.1016/j.cose.2013.12.004		X			X		X	X		X		
72. Mitchell, K. J., Ph, D., Finkelhor, D., Ph, D., Wolak, J., D, J., … Ph, D. (2011). Youth Internet Victimization in a Broader Victimization Context. *Journal of Adolescent Health*, *48*, 128–134.	X				X			X				X

Included and coded papers												
Included papers	Atheoretical (AT)	Atheoretical with	Theoretical	Theory Building	Empirical	Conceptual	Offender	Victim	Motivation	Act	Internet	Other
https://doi.org/10.1016/j.jadohealth.2010.06.009												
73. Mitchell, K. J., Jones, L. M., Finkelhor, D., & Wolak, J. (2013). Child Abuse & Neglect Understanding the decline in unwanted online sexual solicitations for U . S . youth 2000 – 2010 : Findings from three Youth Internet Safety Surveys . *Child Abuse & Neglect*, *37*(12), 1225–1236. https://doi.org/10.1016/j.chiabu.2013.07.002	X				X			X		X		X
74. Mitchell, K. J., Finkelhor, D., & Wolak, J. (2007). Youth Internet Users at Risk for the Most Serious Online Sexual Solicitations. *American Journal of Preventive Medicine*, *32*(6), 532–537. https://doi.org/10.1016/j.amepre.2007.02.001	X				X			X	X	X		
75. Mitchell, K. J., Ph, D., Wolak, J., Finkelhor, D., & Ph, D. (2007). Trends in Youth Reports of Sexual Solicitations , Harassment and Unwanted Exposure to Pornography on the Internet. *Journal of Adolescent Health*, *4*, 116–126. https://doi.org/10.1016/j.jadohealth.2006.05.021	X				X			X				X
76. Mitchell, K. J., Wolak, J., & Finkelhor, D. (2008). Are blogs putting youth at risk for online sexual solicitation or harassment ? . *Child Abuse & Neglect 32*, *32*, 277–294. https://doi.org/10.1016/j.chiabu.2007.04.015	X				X			X				X
77. Mitchel, K. J., Wolak, J., & Finkelhor, D. (2005). Police Posing as Juveniles Online to Catch Sex Offenders : Is It Working ? *Sexual Abuse: A Journal of Research and Treament*, *17*(3), 241–267.	X				X		X	X	X			

Included and coded papers												
Included papers	Atheoretical (AT)	Atheoretical with	Theoretical	Theory Building	Empirical	Conceptual	Offender	Victim	Motivation	Act	Internet	Other
78. Mitchell, K. J., Finkelhor, D., & Wolak, J. (2005). The Internet and Family and Acquaintance Sexual Abuse. *Child Maltreatment*, *10*(1), 49–60. https://doi.org/10.1177/1077559504271917	X				X			X	X			
79. Mitchell, K. J., Finkelhor, D., Wolak, J., Mitchell, K. J., Finkelhor, D., Victimization, J. W., & Wolak, J. (2004). Victimization of Youths on the Internet. *Journal of Aggression, Maltreatment & Trauma*, *8*(1–2), 1–39. https://doi.org/10.1300/J146v08n01	X				X			X		X		X
80. Murumaa-Mengel, M. (2015). Drawing the Threat: A Study on Perceptions of the Online Pervert among Estonian High School Students. *YOUNG*, *23*(1), 1–18. https://doi.org/10.1177/1103308814557395	X				X			X	X			
81. Navarro, J. N., & Jasinski, J. L. (2015). Demographic and Motivation Differences Among Online Sex Offenders by Type of Offense : An Exploration of Routine Activities Theories Demographic and Motivation Differences Among Online Sex Offenders by Type of Offense : An Exploration of Routine Activitie. *Journal of Child Sexual Abuse*, *24*(7), 753–771. https://doi.org/10.1080/10538712.2015.1077363			X		X		X		X			
82. Neto, A. C. D. A., Eyland, S., Ware, J., Galouzis, J., Almeida, A. C. De, Eyland, S., … White, M. (2013). Internet Sexual Offending : Overview of Potential Contributing Factors and Intervention Strategies. *Psychiatry, Psychology and Law*, *20*(2), 168–181. https://doi.org/10.1080/13218719.2011.633328		X				X	X		X		X	

Included and coded papers												
Included papers	Atheoretical (AT)	Atheoretical with	Theoretical	Theory Building	Empirical	Conceptual	Offender	Victim	Motivation	Act	Internet	Other
83. Nielsen, S., Paasonen, S., & Spisak, S. (2015). "Pervy role-play and such": girls experiences of sexual messaging online. *Sex Education*, *15*(5), 472–485. https://doi.org/10.1080/14681811.2015.1048852	X				X			X	X			
84. O'Connell, Rachel. "A typology of child cybersexploitation and online grooming practices." (2003).				X		X	X			X	X	
85. Ong, R. (2006). Internet sex crimes against children : Hong Kong â€™ s response Internet Sex Crimes against Children : Hong Kong ' s Response. *International Review of Law, Computers & Technology*, *20*(1–2), 187–200. https://doi.org/10.1080/13600860600699478	X					X	X					X
86. Palasinski, M. (2014). Computers in Human Behavior The roles of monitoring and cyberbystanders in reducing sexual abuse. *Computers in Human Behavior*, *28*(6), 2014–2022. https://doi.org/10.1016/j.chb.2012.05.020		X			X		X					X
87. Peersman, C., Daelemans, W., & Van Vaerenbergh, L. (2011). Predicting age and gender in online social networks. *International Conference on Information and Knowledge Management, Proceedings*, 37–44. https://doi.org/10.1145/2065023.2065035	X				X		X		X			
88. Philips, F., & Morrissey, G. M. (2004). Cyberstalking and Cyberpredators : A Threat to Safe Sexuality on the Internet. *Convergence*, *10*(1), 66–79.	X					X	X					X

Included and coded papers												
Included papers	Atheoretical (AT)	Atheoretical with	Theoretical	Theory Building	Empirical	Conceptual	Offender	Victim	Motivation	Act	Internet	Other
89. Pranoto, H., Gunawan, F. E., & Soewito, B. (2015). Logistic Models for Classifying Online Grooming Conversation. *Procedia - Procedia Computer Science*, *59*, 357–365. https://doi.org/10.1016/j.procs.2015.07.536		X			X		X			X		
90. Pratt, J. (2009). From Abusive Families to Internet Predators? The Rise, Retraction and Reconfiguration of Sexual Abuse as a Social Problem in Canada. *Current Sociology*, *57*(1), 69–88. https://doi.org/10.1177/0011392108097453		X				X	X		X			
91. Quayle, E., & Cooper, K. (2015). The role of child sexual abuse images in coercive and non-coercive relationships with adolescents: A thematic review of the literature. *Child & Youth Services*, *36*(4), 312–328. https://doi.org/http://dx.doi.org/10.1080/0145935X.2015.1092840	X					X		X		X		
92. Quayle, E., & Newman, E. (2015). The Role of Sexual Images in Online and Offline Sexual Behaviour With Minors. *Current Psychiatry Reports*, *17*(6). https://doi.org/10.1007/s11920-015-0579-8)	X					X	X		X			
93. Quayle, E., & Taylor, M. (2011). Social networking as a nexus for engagement and exploitation of young people. *Information Security Technical Report*, *16*(2), 44–50. https://doi.org/10.1016/j.istr.2011.09.006		X				X	X		X			X
94. Quayle, E., & Taylor, M. (2003). Model of Problematic Internet Use in People with a Sexual Interest in Children. *Cyberpsychology & Behavior Volume*, *6*(1), 95–105.				X	X		X			X	X	

Included and coded papers												
Included papers	Atheoretical (AT)	Atheoretical with	Theoretical	Theory Building	Empirical	Conceptual	Offender	Victim	Motivation	Act	Internet	Other
95. Quayle, E., Allegro, S., Hutton, L., Sheath, M., & Lööf, L. (2014). Computers in Human Behavior Rapid skill acquisition and online sexual grooming of children. *Computers in Human Behavior*, *39*, 368–375. https://doi.org/10.1016/j.chb.2014.07.005				X	X		X			X	X	
96. Quayle, E., Holland, G., Linehan, C., Taylor, M., Quayle, E., Holland, G., … Taylor, M. (2000). The internet and offending behaviour : A case study The Internet and offending behaviour : A case study. Journal of Sexual Aggression ISSN:, 6(1–2), 18–96. https://doi.org/10.1080/13552600008413311		X			X		X			X	X	
97. Quayle, E., Vaughan, M., & Taylor, M. (2006). Sex offenders , Internet child abuse images and emotional avoidance : The importance of values. *Aggression and Violent Behavior*, *11*, 1–11. https://doi.org/10.1016/j.avb.2005.02.005		X				X	X		X			
98. Robilotta, S. A., Calkins Mercado, C., & DeGue, S. (2008). Application of the Polygraph Examination in the Assessment and Treatment of Internet Sex Offenders. *Journal of Forensic Psychology Practice*, *8*(4), 383–393. https://doi.org/10.1080/15228930802199333	X					X	X		X			X

Included and coded papers												
Included papers	Atheoretical (AT)	Atheoretical with	Theoretical	Theory Building	Empirical	Conceptual	Offender	Victim	Motivation	Act	Internet	Other
99. Rogers, P., Wczasek, R., Davies, M., Rogers, P., Wczasek, R., & Davies, M. (2011). Attributions of blame in a hypothetical internet solicitation case : Roles of victim naivety , parental neglect and respondent gender Attributions of blame in a hypothetical internet solicitation case : Roles of victim naivety , parental neglect and respo. *Journal of Sexual Aggression*, *17*(2), 196–214. https://doi.org/10.1080/13552601003664869	X				X		X	X		X		X
100. Schulz, A., Bergen, E., & Schuhmann, P. (2015). Social Anxiety and Loneliness in Adults Who Solicit Minors Online. *Sexual Abuse: A Journal of Research and Treatment*, 1–22. https://doi.org/10.1177/1079063215612440	X				X		X		X			
101. Seto, M. C., & Hanson, R. K. (2011). Introduction to Special Issue on Internet-Facilitated Sexual Offending. *Sexual Abuse: A Journal of Research and Treatment*, *23*(1), 3–6. https://doi.org/10.1177/1079063211399295	X					X	X		X			
102. Seto, M. C., Wood, J. M., Babchishin, K. M., & Flynn, S. (2012). Online solicitation offenders are different from child pornography offenders and lower risk contact sexual offenders. *Law and Human Behavior*, *36*(4), 320.	X				X		X		X			
103. Seto, M. C., Karl Hanson, R., & Babchishin, K. M. (2011). Contact sexual offending by men with online sexual offenses. *Sexual Abuse*, *23*(1), 124-145.)	X				X		X			X		X

Included and coded papers												
Included papers	Atheoretical (AT)	Atheoretical with	Theoretical	Theory Building	Empirical	Conceptual	Offender	Victim	Motivation	Act	Internet	Other
104. Shannon, D. (2008). Online Sexual Grooming in Sweden—Online and Offline Sex Offences against Children as Described in Swedish Police Data. *Journal of Scandinavian Studies in Criminology and Crime Prevention*, *9*(2), 160–180. https://doi.org/10.1080/14043850802450120	X				X		X			X		
105. Sheehan, V., Sullivan, J., Sheehan, V., & Sullivan, J. (2010). A qualitative analysis of child sex offenders involved in the manufacture of indecent images of children A qualitative analysis of child sex offenders involved in the manufacture of indecent images of children. *Journal of Sexual Aggression*, *16*(2), 143–167. https://doi.org/10.1080/13552601003698644		X			X		X		X			
106. Sheldon, K., & Howitt, D. (2008). Sexual fantasy in paedophile offenders: Can any model explain satisfactorily new findings from a study of Internet and contact sexual offenders? *Legal and Criminological Psychology*, *13*, 137–158. https://doi.org/10.1348/135532506X173045		X			X		X		X			
107. Sinclair, R., Duval, K., Fox, E., Sinclair, R., Duval, K., & Fox, E. (2015). Child & Youth Services Strengthening Canadian Law Enforcement and Academic Partnerships in the Area of Online Child Sexual Exploitation : The Identification of Shared Research Directions Strengthening Canadian Law Enforcement and Academic Partnerships in. *Child & Youth Services*, *36*(4), 345–364. https://doi.org/10.1080/0145935X.2015.1096588	X					X	X					X

Included and coded papers												
Included papers	Atheoretical (AT)	Atheoretical with	Theoretical	Theory Building	Empirical	Conceptual	Offender	Victim	Motivation	Act	Internet	Other
108. Slane, A. (2011). Luring Lolita : the age of consent and the burden of responsibility for online luring. *Global Studies of Childhood*, *1*(4), 354–364.		X				X	X			X		X
109. Staksrud, E. (2013). Online grooming legislation : Knee-jerk regulation ? *European Journal of Communication*, *28*(2), 152–167. https://doi.org/10.1177/0267323112471304		X			X			X				X
110. Surjadi, B., Bullens, R., Horn, J. Van, Bogaerts, S., Surjadi, B., Bullens, R., … Bogaerts, S. (2010). Internet offending : Sexual and non-sexual functions within a Dutch sample Internet offending : Sexual and non-sexual functions within a Dutch sample. *Journal of Sexual Aggression*, *16*(1), 47–58. https://doi.org/10.1080/13552600903470054		X			X		X		X			
111. Tener, D., Wolak, J., & Finkelhor, D. (2015). A Typology of Offenders Who Use Online Communications to Commit Sex Crimes Against Minors A Typology of Offenders Who Use Online. *Journal of Aggression, Maltreatment & Trauma*, *24*(3), 319–337. https://doi.org/10.1080/10926771.2015.1009602				X	X		X			X		
112. Tomak, S., Weschler, F. S., Ghahramanlou-holloway, M., Virden, T., Nademin, M. E., Tomak, S., … Nademin, M. E. (2009). An empirical study of the personality characteristics of internet sex offenders An empirical study of the personality characteristics of internet sex offenders. *Journal of Sexual Aggression*, *15*(2), 139–148. https://doi.org/10.1080/13552600902823063	X				X		X		X			

Included and coded papers												
Included papers	Atheoretical (AT)	Atheoretical with	Theoretical	Theory Building	Empirical	Conceptual	Offender	Victim	Motivation	Act	Internet	Other
113. Urbas, G. (2010). Protecting Children From Online Predators : The Use of Covert Investigation Techniques by Law Enforcement. *Journal of Contemporary Criminal Justice*, *26*(4), 410–425. https://doi.org/10.1177/1043986210377103	X					X	X			X		X
114. Wachs, S., Wolf, K. D., & Pan, C. (2012). Cybergrooming : Risk factors , coping strategies and associations with cyberbullying. *Psicothema*, *24*(4), 628–633.	X				X			X	X			
115. Wakeling, H. C., Howard, P., & Barnett, G. (2011). Comparing the Validity of the RM2000 Scales and OGRS3 for Predicting Recidivism by Internet Sexual Offenders. *Sexual Abuse: A Journal of Research and Treatment*, *23*(1), 146–168. https://doi.org/10.1177/1079063210375974		X			X		X			X		X
116. Wall, G. K., Pearce, E., Mcguire, J., Wall, G. K., Pearce, E., & Are, J. M. (2011). Are Internet offenders emotionally avoidant ? *Psychology, Crime & Law*, *17*(5), 381–401. https://doi.org/10.1080/10683160903292246		X			X		X		X			
117. Vartapetiance, A., & Gillam, L. (2014). " Our Little Secret " : pinpointing potential predators. *Security Informatics 2014, 3*(3), 1–19.		X			X		X			X		X
118. Wells, M., & Mitchell, K. J. (2007). Youth Sexual Exploitation on the Internet : DSM-IV Diagnoses and Gender Differences in Co-occurring Mental Health Issues. *Child and Adolescent Social Work Journal*, *24*(3), 235–260. https://doi.org/10.1007/s10560-007-0083-z	X				X			X	X			

Included and coded papers												
Included papers	Atheoretical (AT)	Atheoretical with	Theoretical	Theory Building	Empirical	Conceptual	Offender	Victim	Motivation	Act	Internet	Other
119. Wells, M., & Mitchell, K. J. (2008). How Do High-Risk Youth Use the Internet ? Characteristics and Implications for Prevention. *Child Maltreatment*, *13*(3), 227–234. https://doi.org/10.1177/1077559507312962	X				X			X	X			
120. Wells, M., & Mitchell, K. J. (2014). Patterns of Internet Use and Risk of Online Victimization for Youth With and Without Disabilities. *The Journal of Special Education 2014, 48*(3), 204–213. https://doi.org/10.1177/0022466913479141	X				X			X	X			
121. Whittle, H., Hamilton-Giachritsis, C., & Beech, A. (2014). "Under His Spell": Victims' Perspectives of Being Groomed Online. *Social Sciences*, *3*(3), 404–426. https://doi.org/10.3390/socsci3030404	X				X			X		X		
122. Whittle, Helen C., Catherine Hamilton-Giachritsis, and Anthony R. Beech. "Victims' voices: The impact of online grooming and sexual abuse." *Universal Journal of Psychology*1.2 (2013): 59-71.	X				X		X	X		X		X
123. Whittle, H. C., Hamilton-Giachritsis, C. E., & Beech, A. R. (2015). A Comparison of Victim and Offender Perspectives of Grooming and Sexual Abuse. *Deviant Behavior*, *36*(7), 539–564. https://doi.org/10.1080/01639625.2014.944074	X				X		X	X		X		
124. Whittle, Helen, et al. "A review of online grooming: Characteristics and concerns." *Aggression and violent behavior* 18.1 (2013): 62-70.		X				X		X		X	X	
125. Whittle, Helen, et al. "A review of young people's vulnerabilities to online grooming." *Aggression and violent behavior* 18.1 (2013): 135-146.	X					X		X	X		X	

Included and coded papers												
Included papers	Atheoretical (AT)	Atheoretical with	Theoretical	Theory Building	Empirical	Conceptual	Offender	Victim	Motivation	Act	Internet	Other
126. Williams, M. L., & Hudson, K. (2013). Public perceptions of internet , familial and localised sexual grooming : Predicting perceived prevalence and safety Public perceptions of internet , familial and localised sexual grooming : Predicting perceived prevalence and safety. *Journal of Sexual Aggression*, *19*(2), 218–235. https://doi.org/10.1080/13552600.2012.705341	X				X		X			X		X
127. Williams, R., Elliott, I. A., Beech, A. R., (2013). Identifying Sexual Grooming Themes Used by Internet Sex Offenders Internet Sex Offenders. *Deviant Behavior*, *34*(2), 135–152. https://doi.org/10.1080/01639625.2012.707550				X	X		X			X		
128. Wolak, Janis, et al. "Online" predators" and their victims: myths, realities, and implications for prevention and treatment." *American psychologist* 63.2 (2008): 111.	X					X	X	X	X		X	
129. Wolak, J., Finkelhor, D., & Mitchell, K. (2004). Internet-initiated sex crimes against minors: Implications for prevention based on findings from a national study. *Journal of Adolescent Health*, *35*(5), 424-e11.	X				X			X	X			
130. Wolak, Janis, and David Finkelhor. "Are crimes by online predators different from crimes by sex offenders who know youth in-person?." *Journal of Adolescent Health* 53.6 (2013): 736-741.	X				X		X		X			
131. Wolfe, S. E., & Higgins, G. E. (2008). College Students' Punishment Perceptions of Online Solicitation of Children for Sex. *American Journal of Criminal Justice*, *33*(2), 193–208. https://doi.org/10.1007/s12103-008-9039-x	X				X		X			X		X

Included and coded papers												
Included papers	Atheoretical (AT)	Atheoretical with	Theoretical	Theory Building	Empirical	Conceptual	Offender	Victim	Motivation	Act	Internet	Other
132. Yang, D. W., & Donahue, P. A. (2007). Protecting Children from Online Exploitation and Abuse : An Overview of Project Safe Childhood Protecting Children from Online Exploitation and Abuse : An Overview of Project Safe Childhood *. *Pepperdine Law Review Volume*, *34*, 439.	X					X	X			X		X
133. Yar, M. (2013). The policing of Internet sex offences : pluralised governance versus hierarchies of standing. *An International Journal of Research and Policy*, *23*(4), 482–497. https://doi.org/10.1080/10439463.2013.780226	X					X	X			X		X
134. Ybarra, M. L., Espelage, D. L., & Mitchell, K. J. (2007). The Co-occurrence of Internet Harassment and Unwanted Sexual Solicitation Victimization and Perpetration : Associations with Psychosocial Indicators. *Journal of Adolescent Health*, *41*, S31–S41. https://doi.org/10.1016/j.jadohealth.2007.09.010	X				X			X	X			
135. Young, K. S. (2008). Internet Sex Addiction Risk Factors, Stages of Development, and Treatment. *American Behavioral Scientist*, *52*(1), 21–37.				X		X	X		X			

APPENDIX 2: Structured coding matrix

Theme	Sub-theme	Description	Example (omitted)	Code Offender	Code Victim
Theme 1 Gaining Access	Introductory messages	Initiating contact	Hi; Hello; Hey; Good morning;	OT1	VT1
	Assessment	Assessing the individual characteristics of the offender; the individual characteristics of the victim/offender regarding potentiality, while getting to know each other; assessing the environment (location, family, and relationships), willingness, and availability; sexuality assessment and assessment of sexual experiences	in which part of <town> do you live?; well what do you want to know about me?; How old are you?; what are your measurements; Well i am going now would it be still possible that you text? :); why are you pleased?; how old was he?; btw.. What is your name? :); have you ever had good sex?; hey what are you going to wear?	OT2	VT2
Theme 2 Gaining compliance	Building rapport	Simulating friendship/romance, coordination, predictability, and stability of behaviors; mutuality—mutual attentiveness and interests; positivity—friendliness, empathy, and warmth, manipulation, overt manipulation, liberal thinking, mirroring	i am tall and hot would you like this kind of a lovely guy :); well yes.. But i am not much brave and fun ..; i have never really met people from the internet; i am just depressed cause i have school tommroow; somewho i am really excited to get to high scool..there is no stupid homework; are we together now?	OT3	VT3
Theme 3 Sexual abuse	Sexting	Exchange of text messages with sexually explicit or sexually implicit content and/or context	do you like shaved and a big cocks?; I am jerking off; I want you to like my pussy; i am a bit horny; i got cum in my mouth today.	OT5	VT5
	Producing, distributing, possessing Child	Requests for/or creation, exchange, and distribution of child abusive material (CAM) (exchange of images, video).	i can send you a pic when you come back; can you send me some hot	OT6	VT6

Theme 3 (Continued)	Abuse Material (CAM)		picture; can you send me a naked video;		
	Streaming	Requests for/or creation, exchange, and distribution of child abusive material (CAM) (exchange of images, video).	can we see through skype; can I call you with camera; can you show yourself on cam.	OT7	VT7
	Physical Abuse Potential	Assessing the potential and possibility for a meeting in the physical world, discussing previous meetings in the physical world	can we meet as friends; can we meet tomorrow; do you want to see me; what are you doing Friday, can we meet?; last night was crazy; would you meet me again?;did you get a ticket for the train; we can meet in this hotel.	OTX	VTX
Theme 4 Maintenance	Assessing risk	Assessing the likelihood of activities being detected by, for example, the child's parent(s), guardian, older siblings, or law enforcement	I don't want anyone to see us; what would your mum say; is your brother in the room; try to have the screen behind them: can you go udner your blanket to talk;	OT8	VT8
	Control and Harassment	Bribery, gifts, money, force, and threats, integrity projection, suffering, insidious controlling, intimidation and fear, blackmail	I can send you some money; I can buy you something nice: would you buy me cigarettes for me and my friend; do you want some alcohol;	OT9	VT9

APPENDIX 3: Unconstrained coding matrix

Affordances code sheet – Unstructured coding matrix				
Primary Affordance conceptualization	**Occurring Sub-affordances**	**Description**	**Example**	**Code**
Cyber ID Expressing and discussing identity related parameters	Name	Discussing actors names	whats your name; whats your surname; well you know her name or smth?	x1(1)
	Age	Discussing actors age	how old are you?; is my age a bad thing?	x1(2)
	Gender	Discussing actors gender	are you a girl or a boy; sex?	x1(3)
	Location	Discussing actors location	where do you live?; are you from <town>?; well i can come to the <town>?	x1(4)
	Social status	Discussing actors social status	are u single?; I am not in a realtionship; is she married or smth?	x1(5)
	Nicknames	Discussing actors nicknames	Whats your nickname?; I don't see your nickname anymore;	x1(6)
Cyber Presence Online manifestation of identity related parameters	Photos	Discussing photos	do you have pictures?; You like my picture?; I want a nice pic of you ::) ;	x2(1)
	Videos	Discussing videos	can i see you?; can we see through Skype?	x2(2)
	Voice/call	Discussing calls or voice messages	can I call you?; can you give me your phone number so I can call you?	x2(3)
	Platforms	Discussing digital platforms	do you have pictures somewhere else?; can you send me a link to your profile on fb?	x2(4)

Affordances code sheet – Unstructured coding matrix				
Primary Affordance conceptualization	**Occurring Sub-affordances**	**Description**	**Example**	**Code**
Cyber Presence (Continued*)	Links	Discussing links	send me a link!; <youtube link>; <social media platform link>	x2(5)
	Texts	Discussing texts	can you text me on <phone number>; too bad that u dont want to text or smth ; and u dont answer text messages and so on	x2(6)
Cyber Time Online status and a-synchronized online presence	Online status	Discussing online status	I will be right back; away from pc; I will not be on my computer now	x3(1)
	Previous message in chat	Referring to previous message in chat in the current chat	You didnt answer the other one ; i hope you didnt get mad when i asked that question?	x3(4)
	Previous call/sms out of chat	Referring to previous call/sms exchanged outside the chat	hey it was nice to talk on the phone :); Was the thing i said on phone somehow funny or weird? :); so are you interested for what I said in the sms?	x3(5)
	Previous meeting experience for both actors	Referring to previous real life experience for both actors when they have actually met	every time you see me you are really happy; yesterday was fun.	x3(6)
Cyber Fantasy Abstract image construction (imaginative state) achieved through online text exchange	Explicit Fantasy	Expressing imaginative states with explicit sexual content	I really wanna fuck you; i like to finger and lick its the best; well i can make people come with my dick;	x4(1)
	Passive Fantasy	Expressing imaginative states with implicit or non-explicit sexual content	you sound like a dream :); in what way pervy?; hey what are you going to wear?; well i am not horny at all ; have you had anyone else during my time?; what did you do when you went in his car?; did you go all the way?; so hot;	x4(2)

Affordances code sheet – Unstructured coding matrix				
Primary Affordance conceptualization	**Occurring Sub-affordances**	**Description**	**Example**	**Code**
Cyber Fantasy (Continued*)	Suggestive Fantasy	Expressing imposture of an imaginative state, hinting towards passive or explicit imaginative states	I would really like to that with you; I would love that; that will drive me mad; well you are pretty fun age; meaning that we can get to know each other better; . I should be on your mind :); something racy and sexy;	x4(3)
	Non-Malicious Fantasy	Expressing construction of imaginative states that do not contain explicit, implicit or suggestive sexual imaginative states. Image construction of miscellaneous nature.	i am a handsome guy; I was at school; I have a motorbike; if we would meet we would have so much fun; tell me something about yourself; I am tall and brown eyes;	x4(4)
Cyber Synchronization Towards stability and assessing potential of practicing imaginative states (leveling of the minds of the actors in the communication)	Seeking approval	Seeking approval towards an imaginative state/a request towards imaginative state usually expressed as a question that invites construction of an imaginative state.	tell me more?; hi, tell me anything :); can you do that for me?; will you (…)?;what are you going to wear?; why don't you (…)?	X5(1)
	Expressing approval	Expressing approval towards an imaginative state, usually expressed as compliance, agreement or confirmation to seeking approval, or stand-alone positive statement in regard of the image creation invitation	hi; yeah; yes; no; why not; i dont :D; sorry :); yes you can call; lovely; would be loveley; of course i want to; abosloutely; but i want to;	X5(2)
	Neutrality	Neutrality, doubt or insecurity towards construction of imaginative states usually expressed as neither	maybe; i dont think i got you; you dont have to; wait a moment; aaaaah; yeah;	X5(3)

Affordances code sheet – Unstructured coding matrix				
Primary Affordance conceptualization	**Occurring Sub-affordances**	**Description**	**Example**	**Code**
Cyber Synchronization (Continued*)		compliance or image invitation, but neutral statement towards the imaginative state discussed	haha you are funny now; ….; just because; i dont know;	
	Dismissal	Dismissal of, or non-compliance to imaginative states discussed or asked, denying construction of imaginative states.	no; i cant tell you where i live; dont call me; i cant meet tommorow; i dont; i wont say; cant be bothered to talk; i havent met anyone; sorry; i cant on my phone; i cant send it; well i am not going there.	X5(4)
	Mirroring	Complete agreement between two constructed imaginative states between the actors	hah me too; same here; i have work too; i am bored as well;	X5(5)
	Manipulation	Construction of an imaginative state aimed to change one's attitude towards another imaginative state, usually expressed as compliment, suspenseful reaction, and "sugar-coating".	i thought you were nice and pleasent, but you answer with just one word, really boring; Are you brave or a nerd?; you are nice and brave; whats the bravest thing you have done;	X5(7)
	Imperative/Force	Imperative imposture of an imaginative state/a command for adopting a suggested imaginative state, usually expressed as forceful language.	say!; tell me!; answer!; call me allready; call me now!; because I say so!;	X5(9)
	Aggression	Aggressive imposture of an imaginative state/ an aggressive command for adopting a suggested imaginative state, usually expressed through threats or insults.	fuck you are stupid; i will come and kill you; dont ask it fucking annoys me; cause i am fucking telling you!;	X5(10)

Affordances code sheet – Unstructured coding matrix				
Primary Affordance conceptualization	**Occurring Sub-affordances**	**Description**	**Example**	**Code**
Cyber Synchronization (Continued*)	Break of contact	Constructing imaginative states towards breaking the contact or the synchronization, usually expressed as unavailability of further practice of imaginative states or leaving the conversation.	i need to go; delete my number if you want; i should go soon; delete me from skype; I go now forever;	X5(11)
	Neutralization	Constructing imaginative states that served to neutralize any negative polarization towards the suggested imaginative states within the chat	you wanted it yourself; Cause i had much more fun now, when i wanted it myself :D; cause you have met other older people.; age is just a number; if we have fun it shouldn't matter:	X5(13)
Cyber Control Evaluating risks for the established relationship or exchanged communication in regard of law enforcement or social control, risk awareness, trust control.	Law enforcement control	Discussing law enforcement control in regard of imaginative states or the formed relationship	I can report you; you should be in jail; I can call the police;	X6(1)
	Social Control	Discussing social control in regard of imaginative states or the formed relationship	are you alone right now what are you doing?; what about your parents; what are you going to say to your folks if we would meet?; that my little brother is sleeping in the next room; cause they can see us;	X6(2)
	Risk Awareness	Expressing awareness of the possible negative outcomes of the information exchanged, or the general wrongness of the formed relationship	yeah i know i am a lot younger than you; is my age an issue?;you ask all that shit and talk to a 13 y.o that's sick; well and you are young and illegal, even better :); i fucking know everything that is happening out there!; I can report you to Fobba you are a pedo;	X6(3)

Affordances code sheet – Unstructured coding matrix				
Primary Affordance conceptualization	**Occurring Sub-affordances**	**Description**	**Example**	**Code**
Cyber Control (Continued)	Trust Control	Evaluation of the risk for disclosure of discussed imaginative states or formed relationship	you told anyone about me?; can I really trust you?; are you trustworthy?; can I really be open with you?; you shouldn't say anything about this; i wont tell anyone;	x6(7)

APPENDIX 4: Random effects and logistic regression

In this section, I present the panel data regression analysis of the affordances used in the various chats. The random-effects logistic analysis of the qualitative codes of the cyber affordances provides the likelihood of a sub-affordance code occurring in the same line as the sub-affordance code of interest, while the logistic regression analysis provides the likelihood of certain sub-affordances predisposing the occurrence of the sub-affordance of interest. This exploration is provided as an appendix due to the limited generalizability of the logistic regression, due in turn to the small sample size of only 14 victims who varied in the data sample. However, it is included as auxiliary material, since the data set contained 12,900 data entries, or chat lines, with their assigned qualitative codes in STATA. At its core, this endeavor contributes toward illustrating the potential of performing such analysis on chat logs in the future. With this, I strive to answer the following questions:

1. Which sub-affordance is most likely to occur in the same line in which the victim is expressing risk awareness in the various chats?
2. Which sub-affordances predispose the victim's break of contact in the various chats?
3. Which sub-affordances are most likely to occur in the same line in which explicit fantasy is being used?
4. Which sub-affordances are most likely to predispose the victim's agreement to send a picture to the offender?
5. Which sub-affordances are most likely to predispose the victim's agreement to meet the offender?

1. Which sub-affordance is most likely to occur in the same line in which the victim is expressing risk awareness in the various chats?

The results show that chat length increases the likelihood that the victim will become aware of being abused (Table 5). It is very likely that the victim's risk awareness is related to the use of age in the context of cyber identity. This means that a victim might be more likely to become aware of the abuse when discussing the age issue in the "relationship." The recommendation here would be to educate victims to press the offender to validate his age and to be mindful if they are communicating with a chat partner who is overly emphasizing age-related issues. It is also very likely that this it when, in the same line, dismissal, manipulation, imperative/force, aggression, neutralization, and break of contact are being used from the cyber synchronization affordance. This means that when the conversation seems to be gaining negative polarization, the victim might be more likely to express risk awareness in relation to that negative polarization. This can be informative for the future development of prevention material.

Risk awareness is also very likely to occur in relation of using law enforcement from the cyber control affordance. It is interesting that the victims seemed to be more likely to express risk awareness at the same time that they

used law enforcement control, even though the risk awareness remained silent on the parallel use of social control. This means that when victims are risk aware, they might threaten the offender by reporting him to the police rather than threatening him with disclosing their contact or relationship to their parents. Educational polices should be strengthened in terms of developing trust between youth behavior online and their parents or guardians. Victim risk awareness is also likely to occur in reference to nicknames and links. This is a slightly less significant relationship, yet it occurred that this offender was recruiting victims by acquiring different nicknames and links from their social media profile. In these chats, a relationship might occur when victims are likely to express risk awareness in relation to the offender's recruitment process. It is least likely that risk awareness will occur in the same line when location is used from cyber identity; when calls, video, and platforms are used from cyber presence; and when explicit, passive, and non-malicious fantasy are used from cyber fantasy. This means that victims might be unaware of the risk, especially when they use location, when they practice their online presence habits, and when they engage in cyber fantasy. Specific measures should be taken to educate victims about safe practices in terms of sharing their location and online presence habits, such as safe practice in sexting and using voice and calling services.

Table 5: Sub-affordances used in the same line as risk awareness by the victim

Dependent variable: Risk awareness in victim		
	Occurrence of sub-affordances in the same line	
	Chat length	0.000550***
		(6.06)
Cyber ID	Name	0.848
		(1.33)
	Age	2.400***
		(14.52)
	Location	-0.932***
		(-3.83)
	Social status	-0.225
		(-0.27)
	Nicknames	1.099**
		(2.33)
Cyber Presence	Photos	-0.0549
		(-0.18)
	Video	-3.470***
		(-2.77)
	Voice/Call	-1.826***
		(-5.17)
	Platforms	-0.944***
		(-2.69)
	Links	0.996**
		(2.17)
	SMS	-0.256

Cyber time		(-0.20)
	Online status	0.445
		(0.33)
	Previous message in chat	0.0667
		(0.07)
	Previous SMS/call outside of chat	-0.4
		(-0.32)
	Previous meeting experience for both	-0.094
Cyber Fantasy		(-0.16)
	Explicit fantasy	-1.239***
		(-3.31)
	Passive fantasy	-1.378***
		(-6.65)
	Suggestive fantasy	-0.0439
		(-0.21)
	Non-malicious fantasy	-0.991***
		(-6.59)
Cyber Synchronization	Seeking approval	-0.0362
		(-0.24)
	Expressing approval	-0.183
		(-1.10)
	Neutrality	0.126
		(0.68)
	Dismissal	0.351**
		(2.03)
	Mirroring	0.879
		(0.7)
	Manipulation	0.882***
		(5.39)
	Imperative/Force	1.323***
		(2.64)
	Aggression	0.681***
		(4.94)
	Break of contact	0.669*
		(1.91)
	Neutralization	1.144***
Cyber Control		(4.19)
	Law enforcement	2.852***
		(4.06)
	Social control	0.126
		(0.29)
	Trust control	0.117
		(0.11)
	Constant	-3.420***
		(-12.41)
	Number of observations	5017
*Variation in parentheses; *** p < 0.01, ** p < 0.05, * p < 0.1.*		

2. **Which sub-affordances predispose the victim's break of contact in the various chats?**

The chat lengths seem to be negatively correlated with the occurrence of break of contact. The most significant relationships show that the victim was more likely to use break of contact from the cyber synchronization affordance, when, in the previous lines, there was use of force/intimidation and aggression from cyber synchronization and use of risk awareness from cyber control (Table 6). It is less likely that break of contact will be used when non-malicious fantasy is used in the previous lines. Perhaps, the victims did not feel the need to break contact when random imaginative states were being discussed, yet it appears that they did not feel a need to break contact, even when, for example, the non-malicious fantasy escalated into explicit fantasy. Educative measures should be taken to help children develop defense mechanisms triggered by the use of aggression or force in the chat.

Table 6: Sub-affordances used in the previous line from break of contact

Dependent variable: victim's break of contact	**Occurrence of sub-affordances in previous lines**	
	Chat length	-0.000351***
		(-2.62)
Cyber ID	Age	0.196
		-0.56
	Location	-0.585*
		(-1.78)
	Social status	0.347
		-0.33
Cyber Presence	Photos	-0.84
		(-1.53)
	Video	-1.26
		(-1.22)
	Voice/Call	-0.196
		(-0.58)
Cyber Time	Previous call/message outside of chat	1.370*
		-1.79
Cyber Fantasy	Explicit fantasy	-0.231
		(-0.55)
	Passive fantasy	-0.284
		(-0.88)
	Suggestive fantasy	0.327
		-1.05
	Non-malicious fantasy	-0.662***
		(-2.75)

Dependent variable: victim's break of contact Occurrence of sub-affordances in previous lines		
Cyber Synchronization	Seeking approval	-0.327
		(-1.51)
	Expressing approval	0.0533
		-0.19
	Neutrality	0.00329
		-0.01
	Dismissal	0.184
		-0.63
	Manipulation	0.0676
		-0.28
	Force/Intimidation	1.539***
		-2.81
	Aggression	0.945***
		-6.44
Cyber Control	Law enforcement	1.419
		-1.19
	Social control	-0.255
		(-0.46)
	Risk awareness	0.991***
		-2.7
	Constant	-3.360***
		(-9.16)
	Number of observations	4468
	*Omitted variables not shown *Variation in parentheses; *** p < 0.01, ** p < 0.05, * p < 0.1.*	

3. Which sub-affordances are most likely to occur in the same line in which explicit fantasy is being used?

Explicit cyber fantasy is most likely to occur in the same line as previous meeting experience and passive fantasy (Table 7). It is also most likely to occur when imperative/force and aggression are being used and likely when dismissal is used from cyber synchronization in the same line. Videos are also likely to be discussed when explicit fantasy is active. It is less likely that explicit fantasy is used in the same line as all the cyber ID sub-affordances: when calls or platforms are being used from cyber presence; break of contact from cyber synchronization; suggestive fantasy from cyber fantasy; and social control and risk awareness from cyber control.

The results also show that explicit fantasy was used in the same line with previous meeting experience and passive fantasy for both actors. This is a worrisome finding, since it might be that the offender in these cases is likely to

be highly skilled and uses explicit fantasy very often after he has abused the victim in the physical world. It also means that he continues to support the explicit imaginative state by using implicit language that does not contain any sexually explicit words. He seems to be very cautious about not using explicit language when the victim is using risk awareness, engages in an assessment of cyber ID, or peruses to establish cyber presence. Again, this is a worrisome finding in terms of prevention methods that concentrate on detecting sexual explicitness as a means of preventing cyber grooming; when dealing with offenders such as this one, the abusive language might not be detected until the offender meets his victim in the physical world. Perhaps after a physical abuse incident, the offender feels safe to use explicit fantasy, or even worst, he feels that the victim is already trapped in the abuse cycle and that there is a slimmer chance that she/he will report him.

Table 7: Sub-affordances used in the same line with explicit fantasy

Dependent variable: explicit fantasy in offender and victim		
	Occurrence of sub-affordances in the same line	
	Chat length	0.000172***
Cyber ID		(3.99)
	Name	-2.023***
		(-3.21)
	Age	-0.738***
		(-6.19)
	Location	-0.850***
		(-6.22)
	Social status	-1.051*
		(-1.68)
	Nicknames	-2.336**
		(-2.26)
Cyber Presence	Photos	-0.0859
		(-0.34)
	Video	0.600**
		(1.98)
	Voice/Call	-2.316***
		(-4.84)
	Platforms	-1.605***
		(-4.29)
	Links	-0.158
		(-0.15)
	SMS	-0.811
		(-0.78)
Cyber time	Online status	-0.117
		(-0.11)
	Previous message in chat	-0.584
		(-0.76)
	Previous message/SMS outside of chat	-1.489

Dependent variable: explicit fantasy in offender and victim		
	Occurrence of sub-affordances in the same line	
		(-1.46)
	Previous meeting experience for both actors	1.674***
		(8.34)
Cyber Fantasy	Passive fantasy	2.122***
		(23.37)
	Suggestive fantasy	-0.831***
		(-4.82)
	Non-malicious fantasy	0.0323
		(0.29)
Cyber Synchronization	Seeking approval	-0.0604
		(-0.76)
	Expressing approval	0.0398
		(0.41)
	Neutrality	-0.141
		(-1.07)
	Dismissal	0.290**
		(2.56)
	Mirroring	0.478
		(0.99)
	Manipulation	-0.0383
		(-0.33)
	Force/Intimidation	0.953**
		(2.38)
	Aggression	0.269***
		(2.9)
	Break of contact	-1.000***
		(-2.68)
	Neutralization	0.187
		(0.9)
Cyber control	Law enforcement	1.224
		(1.15)
	Social control	-0.809**
		(-1.99)
	Risk awareness	-1.155***
		(-4.25)
	Trust control	0.789
		(0.76)
	Constant	-5.571***
		(-7.79)
	Number of observations	12950
	Variation in parentheses; $***p < 0.01$, $**p < 0.05$, $*p < 0.1$.	

4. **Which sub-affordances are most likely to predispose the victim's agreement to send a picture to the offender?**

First, the chat length seems to increase the likelihood that the victim is going to send a picture. It is more likely that a victim will send a picture in the chats where: name and age are heavily used from cyber ID and where there is a heavy use of photos and some use of calls from cyber presence (Table 8). This might mean that the offender's persistence over time of repetitively asking for a picture from the victim can result in the victim yielding in compliance. The results depicting a heavy use of the cyber ID sub-affordances, such as name and age, might mean that the offender is requesting pictures from the victim's peers. A recommendation here is for a detective software to be able to detect the use of names, nicknames, and age, for example: *"she is 13."*

The victims also seemed to send a picture when manipulation, imperative/force, and aggression were heavily deployed from cyber synchronization. The heavy use of the "negative" cyber synchronization sub-affordances (manipulation, imperative/force and aggression) perhaps also complemented the offender's persistence. There was also a significant relationship with all the social control affordances and a slightly less significant relationship with the use of trust control and risk awareness. This might mean that in chats where the victim has sent a picture, the offender was super careful in assessing whether social control was present around the victim and continuously worked on trust maintenance. It might also mean that risk awareness was used when the victims were sending a picture, which might explain the use of the law enforcement sub-affordances.

Conversely, it is less likely that the victim sent a picture when explicit fantasy, seeking approval, and neutralization were heavily utilized. This might be interpreted as the offender "not needing" a picture in chats where explicit fantasy was used or that his predatory needs were being satisfied through a different cyber medium or affordance. Nevertheless, to explain the negative correlation between the victim sending a picture with the use of the seeking approval and neutralization sub-affordances, one can argue that since the victim had sent the pictures, use of neutralization was not needed. This is particularly so when considering that neutralization is positively associated as a predisposition before break of contact or when it simultaneously occurs with the victim's risk awareness. It might be that the offender is using neutralization as a last resort when he feels that that the victim is not complying with his intentions. It is also less likely that the victim will send a picture when his/her online status is being used. Online status is usually used when the offender is assessing whether the victim is online or when the victim suddenly disappears from the chat. The conclusion might be that the victim is not "committed" to replying continuously to the offender and is less likely to send a picture.

Table 8: Most frequent sub-affordances in the chats where the victim has sent a picture

Dependent variable: victim has sent a picture		
	Most frequent sub-affordances in the chats	
	Chat length	0.00205***
		(2.92)
Cyber ID	Name	1.595***
		(3.91)
	Age	0.499***
		(3.66)
	Location	-0.226
		(-1.35)
	Social status	-0.352
		(-0.70)
	Nicknames	0.151
		(0.26)
Cyber Presence	Photos	2.104***
		(5.88)
	Videos	1.011*
		(1.67)
	Voice/Call	0.879*
		(1.77)
	Platforms	-0.3
		(-0.75)
	Links	0.763
		(0.53)
	SMS	-0.237
		(-0.22)
Cyber time	Online status	-2.387**
		(-2.21)
	Previous message in chat	0.412
		(1.26)
	Previous message or SMS outside of chat	0.574
		(0.75)
	Previous meeting experience for both actors	-1.42
		(-0.92)
Cyber Fantasy	Explicit fantasy	-1.325***
		(-2.66)
	Passive fantasy	0.205
		(0.87)
	Suggestive fantasy	-0.202
		(-1.00)
	Non-malicious fantasy	-0.237
		(-1.14)
Cyber Synchro	Seeking approval	-0.309**
		(-2.41)
	Expressing approval	0.00376

Dependent variable: victim has sent a picture		
	Most frequent sub-affordances in the chats	
		(0.03)
	Neutrality	0.241
		(1)
	Dismissal	0.0265
		(0.14)
	Mirroring	0.441
		(0.94)
	Manipulation	0.633***
		(2.73)
	Force/Intimidation	1.060**
		(2.41)
	Aggression	0.702***
		(4.18)
	Break of contact	0.873
		(1.45)
	Neutralization	-1.330***
		(-3.05)
Cyber Control	Law enforcement	-1.443*
		(-1.81)
	Social control	0.947**
		(2.34)
	Risk awareness	0.781*
		(1.74)
	Trust control	2.367**
		(2.39)
	Constant	-0.862
		(-1.02)
	Number of observations	12950
	*Variation in parentheses; *** p < 0.01, ** p < 0.05, * p < 0.1.*	

5. Which sub-affordances are most likely to predispose the victim agreement to meet the offender?

It is more likely that a victim will agree to meet with the offender when there is a heavy use of location from the cyber ID affordance (Table 9). This implies that the use of location in online communication is extremely dangerous. I believe that this goes beyond only revealing the location, since the reveal usually happens in the first introductory messages. These days, the sheer extent of social media presence means that it is very difficult not to reveal location. Thus, the results signal that this sub-affordance is predominantly used in relation to the other sub-affordances, which means that the offender is repetitively using this sub-affordance, or he may be constructing his persistence techniques around location if he sees that there is a potential for the victim to meet him.

The victim is also more likely to meet the offender when there is a heavy use of explicit cyber fantasy, previous message in chat, and previous meeting

from the cyber time affordance. This proves that those who met the offender engaged in greater use of explicit fantasy in terms of their meeting.

Further, it is more likely that when the victim agrees to meet the offender, there is a heavy use of aggression, force/intimidation, and break of contact, yet there is a highly significant negative correlation, with the use of risk awareness in the chats, when the victim agrees to meet the offender. Previously, we found that break of contact usually appears after the use of aggression, force/intimidation, and risk awareness. Here, we see a high use of break of contact and no risk awareness. It is my belief that when victims have agreed to meet the offender, the high use of aggression, force/intimidation, and break of contact is more reflective of them feeling intimate and in a "real relationship." Thus, these "negative" cyber synchronization sub-affordances might also occur as "having a fight" rather than a mechanism that forces the victim to meet the offender. Heavy use of nicknames from cyber ID, calls and platforms from the cyber presence affordance, and suggestive fantasy and mirroring from cyber synchronization are negatively correlated with chats in which the victim has agreed to meet the offender. It might be that with victims who do not want to meet the offender, the offender diverts to calling them and/or moves toward recruiting other victims through the heavy use of nicknames and platforms.

Table 9: Most frequent sub-affordances in the chats where the victim has agreed to meet the offender

Dependent variable: victim agreed to meet the offender		
	Most frequent sub-affordances in the chats	
	Chat length	0.000115
		(0.2)
Cyber ID	Name	0.167
		(0.5)
	Age	-0.149
		(-1.45)
	Location	0.831***
		(4.04)
	Social status	0.514
		(1.35)
	Nicknames	-0.970**
		(-2.48)
Cyber Presence	Photos	-0.24
		(-0.73)
	Videos	0.555
		(0.77)
	Voice/Calls	-0.515*
		(-1.84)
	Platforms	-0.784***
		(-8.15)
	Links	-0.166
		(-0.46)

Dependent variable: victim agreed to meet the offender		
	Most frequent sub-affordances in the chats	
	SMS	0.277
		(0.4)
Cyber time	Online status	-0.535
		(-1.61)
	Previous message in chat	1.406***
		(3.59)
	Previous text/SMS message outside of chat	0.343
		(0.84)
	Previous meeting experience for both actors	2.869***
		(7.26)
Cyber Fantasy	Passive fantasy	-0.131
		(-1.00)
	Suggestive fantasy	-0.268*
		(-1.76)
	Non-malicious fantasy	0.276**
		(2.06)
Cyber synchronization	Seeking approval	-0.0339
		(-0.20)
	Expressing approval	0.157
		(1.41)
	Neutrality	-0.0641
		(-0.37)
	Dismissal	-0.116
		(-1.32)
	Mirroring	-0.742***
		(-3.31)
	Manipulation	-0.248
		(-1.28)
	Force/Intimidation	0.51
		(0.86)
	Aggression	0.475**
		(2.37)
	Break of contact	0.815***
		(3.23)
	Neutralization	0.00379
		(0.01)
Cyber Control	Law enforcement	-1.083
		(-1.57)
	Social control	0.166
		(0.48)
	Risk awareness	-1.071***
		(-6.28)
	Trust control	-1.097**
		(-2.54)

Dependent variable: victim agreed to meet the offender		
	Most frequent sub-affordances in the chats	
	Constant	0.139
		(0.16)
	Number of observations	12950
	Variation in parentheses; $***$ p < 0.01, $**$ p < 0.05, $*$ p < 0.1.	