The Past, Present, and Future of Online Child Sexual Exploitation: Summarizing the Evolution of Production, Distribution, and Detection

Bryce Garreth Westlake

Contents

Abstract

The sexual exploitation of children has long been a component of society. With the advent of the Internet, along with advancements of, and accessibility to, media-recording devices, child sexual exploitation material has become even more prevalent globally. This chapter chronicles the evolution of child sexual

B. G. Westlake (✉)
San Jose State University, San Jose, CA, USA
e-mail: Bryce.Westlake@sjsu.edu

T. Holt, A. M. Bossler (eds.), *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, https://doi.org/10.1007/978-3-319-90307-1_52-1

exploitation, beginning in ancient Greece, moving to the impact of the Internet today, and concluding with growing trends. In addition, this chapter examines how child sexual exploitation is addressed internationally, including existing legislation, law enforcement actions, and vigilante justice. Finally, this chapter summarizes how technology has been used to find child sexual exploitation material, and where research and combat tools need to go in order to address the evolving problem.

Keywords
Child sexual exploitation · Child pornography · History · Evolution · Combating · Investigating · Distribution

Introduction

Every day society is reminded of the dangers of being victimized on the Internet through hacking, fraud, malware, etc. However, none garner as much of an emotional response from society as the sexual exploitation and abuse of children. Throughout history, the perceptions and methods in which children are sexually exploited have varied; however, with the advent of the Internet, we have seen a once solitary crime become ever-present within society. The advantages of the Internet have allowed the crime of child sexual exploitation to grow seemingly unabated. As methods for producing and distributing content online improve and evolve, government officials, law enforcement agencies, and nongovernment organizations are forced to adapt laws, create tools, and determine the best strategies for minimizing the crime. While it is impossible to eliminate child sexual exploitation, distribution can be somewhat controlled through partnerships and application of technology advancements.

This chapter begins with defining child sexual exploitation from an academic, advocate, and law enforcement perspective, followed by a global, and legal, perspective. It continues with chronicling the sexual exploitation of children throughout history, bringing us toward today's landscape. Next, it summarizes what we know about the prevalence of child sexual exploitation material (CSEM) distribution, including who are the victims, what is in the content, how it is distributed, where it is hosted, and how it is consumed. The chapter then explains how CSEM is investigated by nations and vigilantes, and the roles of Internet service providers. Next are the databases and tools developed to identify CSEM and how technological advancements will aid with improving detection methods, especially with multimedia (e.g., videos). Branching off from technological-based techniques, the chapter delves into methods for better understanding *how* CSEM is distributed, through social network analysis and *network capital*, to improve target prioritization. The chapter concludes by looking ahead to the not-too-distant future of CSEM production and distribution, focusing on the growth of sexting and self-produced content, and the potential rise of virtual reality and teledildonics.

The Evolution of Child Sexual Exploitation

Defining Child Sexual Exploitation

Commonly referred to by society as child pornography, there has been a movement in the last 10–15 years to change the vernacular to more accurately depict what is *actually* occurring and call it child sexual abuse or child sexual exploitation. This is because content – photographs, videos, generated images (i.e., computer or hand-drawn), audio, or written – routinely depicts sexual assault. In addition, the term child pornography can imply that the victim has some degree of agency in the production of content. As a result, law enforcement, advocacy organizations, and researchers will often use the terms child sexual exploitation and child sexual abuse when referring to child pornography as it correctly removes the notion of agency and asserts the victim's innocence in its production.

From a legal perspective, the term child pornography is still heavily used. However, what that means depends on the country. As of 2016, the International Center for Missing and Exploited Children (ICMEC) reports that 82 of 196 countries have sufficient legislation combating child sexual exploitation, with 35 countries having no legislation (Fig. 1). Of the remaining 79 countries with some legislation, 60 do not define "child pornography." In many countries where a definition does exist, it excludes auditory and written depictions, with some countries not including generated images and videos often used for grooming. Recently, there has been a transition to live depictions through video streaming on devices such as webcams, with a growing percentage of this material being produced and disseminated by the children depicted (Sparks 2016). Currently, few if any countries have legislation in place to deal with self-produced child pornography (Westlake 2018).

Although there is currently no international law pertaining to child sexual exploitation, the United Nations General Assembly approved, in 2000, an optional

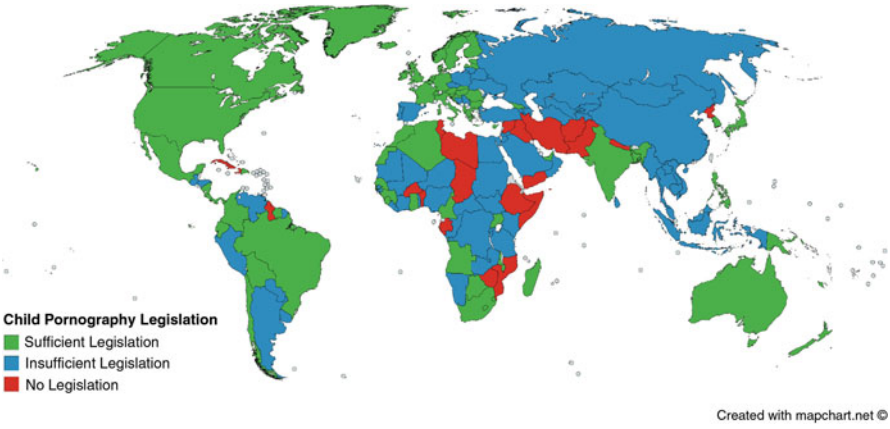

Fig. 1 Legal status of child pornography (child sexual exploitation) around the world. (Based on ICMEC (2016) report)

protocol to the *Convention on the Rights of the Child*. This protocol required that nations prohibit the sale of children, child prostitution, and child pornography. Under the protocol (United Nations 2002), child pornography was defined as "any representation, by whatever means, of a child engaged in real or simulated explicit sexual activities or any representation of the sexual parts of a child for primarily sexual purposes." Entered into force in 2002, this protocol has 121 signatories as of September 11, 2018.

In the United States, child pornography is defined under federal law 18 U.S.C. §2256(8) as any visual depiction, including any photograph, film, video, picture, or computer/computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct. Under 18 U.S.C. §2256(2)(A), sexually explicit is actual or simulated sexual intercourse, whether alone, with another person, or nonhuman. This applies to any person under the age of 18, regardless of the age of consent within the state of the offense. In addition, 18 U.S.C. §2252 prohibits producing, distributing, receiving, or possessing material involving the sexual exploitation of minors. Simulated child pornography, that is child pornography not involving a real child, was temporarily illegal, thanks to the Child Pornography Prevention Act of 1996. Struck down in 2002, in *Ashcroft v. Free Speech Coalition*, it was partly replaced by 18 U.S.C. §1466A, which criminalized visual depictions of a minor that is *both* sexually explicit and obscene or lacks serious value. More recently, the growth in self-produced child pornography, and specifically sexting, has led to calls for amendments to the federal laws to include a "Romeo and Juliet" component for two teenagers consensually exchanging sexually explicit self-pornography. As of September 2018, 25 states had sexting-specific laws with California, Massachusetts, and South Carolina having laws proposed (Hinduja and Patchin 2018). Of the 25, at least 21 have Romeo and Juliet provisions.

In Canada, child pornography is criminalized under Section 163.1 of the Canadian Criminal Code (R.S.C. 1985, c. C-46) and defined as:

> A photographic, film, video, or other visual representation, whether or not made by electronic or mechanical means, that shows a person who is or is depicted as being under the age of eighteen years and is engaged in or is depicted as engaged in explicit sexual activity.

Section 163.1 goes on to state that making, distributing, possessing, and accessing child pornography are also illegal. Since its implementation, two important cases have shaped the current law. The most influential was *R. v Sharpe*, 2001 S.C.C. 2, in which Sharpe argued that his freedom of expression, under Section 2(b) of the Canadian Charter of Rights and Freedoms, was being violated. This brought forth the argument of whether private possession of child pornography, and thus privacy, protected against prosecution. Indirectly, it challenged the line between artistic merit and potential harm to children. The second prominent case was in October 2005, when police arrested Gordon Chin for importing Japanese graphic novels, depicting child pornography. Chin's lawyer argued that he was unaware of the law,

as manga was legal in Japan. This was the first case to prosecute exclusively on manga depiction and not in conjunction with any other laws. Chin was given an 18-month conditional sentence.

Similar cases to those in Canada have cropped up in Australia. In August 2007, a man was fined for attempting to important eight Japanese animations DVDs depicting children under the age of 14 involved in sexual violence. While in December 2008, Alan John McEwan was fined for a pornographic depiction of The Simpsons Bart and Lisa. Finally, in March 2011, a Tasmanian man was convicted for possessing an electronic copy of a nineteenth-century written work *The Pearl*, despite the publication being available for purchase within Australia.

Within Europe, each country develops its own laws. However, due to the European Union, multilateral treaties can be proposed by the Council of Europe (2017). On October 25, 2007, in Lanzarote, Spain, the Council of Europe signed the *Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse* treaty. Under the treaty, child pornography was defined as a child engaged in real or simulated sexually explicit conduct or any depiction of a child's sexual organs for primarily sexual purposes. Signing parties agreed to criminalize certain forms of sexual abuse against children. While the treaty is specific to *only* visual representations (i.e., it excludes audio and written), it does include real and fictitious images. Since coming into force on July 1, 2010, the convention has been ratified by 44 states.

In 2011, the European Union adopted the Directive 2011/93/EU – *combating the sexual abuse and sexual exploitation of children and child pornography*. This Directive was an update to Council Framework Decision 2004/86/JHA, which was unsuccessful in fighting child sexual exploitation due to the explicit sexual conduct proof requirement and the need for the entire framework decision to be present within a nation's legislation for it to be used within the nation's courts. Under the new Directive, in Article 2(c), child pornography is "any material that visually depicts a child engaged in real or simulated sexually explicit conduct." This includes real or simulated sex and realistic images. The Directive also notes "pornographic performances," which include live, audience-based, online streaming performances (e.g., via webcams). Despite providing clearer definitions and stronger protections for victims than its predecessor, Directive 2011/93/EU excludes accidentally entering a website, or not knowing that the website displayed child sexual exploitation material. However, the Directive does address websites circulating CSEM (in Article 25) and advises members to remove CSEM hosted within their territories.

The History of Child Sexual Exploitation

The sexual exploitation of children is not a new phenomenon. In fact, not only has it been prevalent throughout history; it was deemed far more acceptable in the past (Bullough 2004). In ancient Greece, it was common for 12-year-old boys to enter a sexual relationship with other males, around the age of 20. Once the younger boy reached the age of 20, they were usually married to a 12- to 14-year-old girl; at which time they would take on a young male partner of their own to groom. In the Roman

Empire, it was common for girls to get married at the age of 14, while in medieval times, girls as young as 7 were married off. Even at the start of the nineteenth century, in England, it was still legal to have sex with a 10-year-old girl.

The sexualization of youth in art has also been forever present. It was commonly portrayed in Greek and Roman writings, as well as paintings during the Renaissance (Bullough 2004). Popular books such as *Aristotle's Masterpiece* and *Harry's List of Covent Garden Ladies* depicted child sexual exploitation and discussed the "ripe age" of females as being 14 or 15. However, it was the invention of the camera in 1826 that really brought forth our current definition of child sexual exploitation. One of the most notorious early producers of CSEM was Charles Dodgson. Better known as Lewis Carroll, creator of Alice in Wonderland, Dodgson was a prolific photographer and was thought to have produced many pornographic images of girls as young as 6 (Bullough 2004; Jenkins 2001).

The turn of the twentieth century saw a lull in the sexualization of adolescents; however, this was renewed in the 1960s, thanks to increased social liberalization and relaxation of censorship laws and sexual values (Jenkins 2001). The 1970s saw the release of several "classic" child abuse films and more than 250 child sexual exploitation magazines in circulation across the United States, with titles such as *Lolita*, *Broad Street Magazine*, and *Nudist Moppets*. Despite growing interest, CSEM was very expensive to obtain, with magazines imported to the United States selling for $6 to $12 and domestic magazines and videos selling for $25 and $50, respectively (Burgess 1984). In addition, the quality of images in many publications was so poor that the sex of the child was often indiscernible.

Adding to the high cost of acquiring child sexual abuse media, the chances of being apprehended were high. US Customs and US Postal Services claimed to be adept at stemming the flow of imported material. Even if a person was successful in transferring media through the mail, the speed of exchange was low. More importantly, it was difficult for people to get in contact with one another. As a result, prior to the Internet, child sexual exploitation could have been viewed as more of a solitary crime with very sparse networks (Beech et al. 2008). However, the advent of the Internet changed the crime of child exploitation and sexual abuse. The crime became more communal with offenders being able to connect with like-minded individuals around the world. Offenders were able to have 24/7, mostly anonymous and free, instant access, with better quality content and reduced risk of being apprehended (Wortley and Smallbone 2012). As the Internet evolved throughout the 1990s and early 2000s, technology such as search engines, peer-to-peer file sharing, instant messaging, and social networking platforms only further solidified the Internet as the go-to place for CSEM.

Today's CSEM Landscape

Today, the prevalence of CSEM in cyberspace is difficult to accurately quantify as there are so many avenues in which material is distributed, and often the same, or similar, CSEM is distributed under different names. What we do know is that since

creating CyberTipline in 1998, the National Center for Missing and Exploited Children (NCMEC) has received nearly 43 million reports (as of November 20, 2018), and the Child Victim Identification Program has reviewed more than 261 million images and videos and identified more than 15,800 children (Missing Kids 2018).

Analyses have been conducted in Canada, through Cybertip.ca and the Canadian Centre for Child Protection (CCCP 2016); the United Kingdom, through the Internet Watch Foundation (IWF 2016, 2017); and the United States, through NCMEC and Thorn (Seto et al. 2018), which give us some insight into the age and sex of victims, as well as the severity of content and the sex of offenders (Table 1). While each revealed that CSEM was largely consistent of prepubescent girls, CCCP found that explicit and extreme (e.g., sadism and bestiality) sexual assault accounted for a higher volume of material victimizing boys (59.41%) than girls (50.88%) with rates getting higher as the child's age decreased. In children aged 3 or younger, explicit or extreme assault was evident in 59.72% of cases. This was reinforced in IWF's 2017 Annual Report, with 44% of imagery depicting children below 11 being Category A: sexual activity including rape and sexual torture. In comparison, 20% of imagery depicting children aged 11–17 was Category A.

Further findings from the CCCP study revealed that 87.12% of victims were Caucasian, with 7.65% being East/South Asian. Of content involving a sexual act, 53.62% involved adults, 19.83% involved more than one child, and 0.41% involved animals with children. Finally, 68.68% of CSEM was produced in a home, 15.25% outdoors, and 10.81% in a studio. Other common locales were school, pool, change room, shower, gym, vehicle, and tent, which accounted for 5.26% of material. Unsurprisingly, explicit and extreme sexual assault accounted for a larger percentage of content produced at home (69.91%) than outdoors (15.98%) or in a studio (15.51%).

As methods of transmitting files from person-to-person evolved, so too did the peer-to-peer (P2P) preference of offenders. Originally, Internet Relay Chat (e.g., messenger applications) was the go-to method, with Carr (2004) finding that 78% obtained images this way. Since then, we have seen the rise of P2P software, such as Gnutella (Steel, 2009; Wolak et al. 2014), eDonkey (Fournier et al. 2014), and BitTorrent (Rutgaizer et al. 2012).

Despite the growth in P2P networks and Dark Web websites, the Surface Web has always been a popular locale for CSEM. Examining the distribution of CSE images, Carr (2004) identified the World Wide Web (e.g., public websites) as the second most prominent method of acquisition, followed by newsgroups. More recently, O'Halloran and Quayle (2010) conducted a qualitative study of boy love support forums and found that despite public forums being "old technology," they were still being used prominently. Similarly, Tremblay's (2006) study of boy love forums highlighted the use of public spaces for the discussion of illicit activities, such as the distribution of CSEM. Research specifically examining distribution on publicly accessible websites found that free hosting blog services, such as Blogger, LiveJournal, and Tumblr, were heavily relied upon by distributors (Westlake and Bouchard 2016a; Westlake et al. 2017).

Table 1 Characteristics of child sexual exploitation material

Investigator(s)		**CCCP**	**NCMEC and Thorn**		**IWF**	
Timeframe		2008–2015	2011–2014	2011–2014	2016	2017
Cases		43,762	1,965 (1 vs. 1)	633 (multiple off/vic)	57,335 websites	78,589 websites
Age	*Toddlers (~<4)*[a]	7%	6%	3%	2%	2%
	Under 11	72%	33%	31%	53%	55%
	11 and older	22%	61%	42%	45%	43%
Sex	*Boys*	20%	24%	22%	5%	7%
	Girls	80%	76%	62%	89%	86%
Severity	*Sexual posing*	32%	40%	28%	–	–
	Extreme posing	18%	20%	21%	19%	21%
	Explicit sex act	48%	26%	30%	–	–
	Extreme sexual assault	2%	14%	20%	28%	33%
Adults	*Male*	83%	98%	82%	–	–
	Female	17%	2%	3%	–	–

[a]For IWF study, Toddler was <2

Examining which types of websites are most likely to host CSEM, IWF (2017) found that image hosting websites (69%) who allowed images to be embed onto other websites via a URL, and cryptolockers (14%) -third-party file storing and sharing services, such as cloud services (Technopedia 2018)- were the most used hosting services. Comparatively, social media networks accounted for less than 1% of hosted images. Most importantly, 92% of CSEM hosting domains were free-to-use services. Looking specifically at 2,082 self-produced images and videos, across 78 domains, IWF (2018) found that 85% were hosted on image host websites, followed by forums (9%) and cyberlockers (4%).

Although a larger percentage of CSEM is hosted on the Surface Web, it appears that this content is hosted by a relative few. In a 2017 analysis of 130,784 webpages and 43,767 newsgroup posts, IWF found that content was being hosted by only 3,791 domain names. Even more importantly, 87% were hosted in Netherlands (36%), the United States (18%), Canada (15%), France (10%), and Russia (8%). Put another way, a small number of sources, and countries, were hosting CSEM for many websites. In hindsight, this finding may not be too surprising as the November 2018 hacking of Dark Web *Daniel's Hosting* revealed that large numbers of potentially criminal websites are hosted by relative few services (Waqas 2018). For example, in February 2017, anonymous hacked *Freedom Hosting II*, removing a reported 11,000 Dark Web child sexual exploitation websites, accounting for an estimated 20% of CSEM being hosted on the Dark Web at the time.

Increased crackdowns on CSEM in North America (NA) have led to a transition in where content is hosted globally (IWF 2017). In 2015, 57% of content was hosted in NA. By 2017, that number had dropped to 32%. Comparatively, hosting rates in Europe have increased significantly over the same time period. In 2015, 41% of content was hosted in Europe, whereas in 2017 the number had risen to 65%. Despite this, the United States remains one of the largest consumers of CSEM. Examining P2P queries, Steel (2009) found that 29% came from the United States, followed by Malaysia (16%) and Brazil (12%). Following up on his work, Steel (2015) reported that efforts by Google and Microsoft in 2013 to reduce returns of CSEM in web-based searches led to a 67% drop in search volume. Nevertheless, Google is still used by some seeking CSEM, with Czech Republic, Russia, and Mexico leading the way. With popular search engines Google and Bing (Microsoft) removing CSEM from their searches, Steel identified Russia's Yandex as the most sought out alternative, with the largest numbers of searches for CSEM coming from United States, Germany, France, Italy, and the Netherlands.

Like the many ways in which CSEM can be distributed, the ways in which offenders can consume CSEM have also increased. As offenders are often the first to adopt, and exploit, new technology, it is unsurprising that rates of consuming CSEM by mobile devices have increased. Examining devices used to search for CSEM, Steel (2015) found that 34% were conducted from smartphones and tablets. While lower than Steel's findings for adult pornography (48% by mobile device), it is likely that CSEM rates will continue to rise and come in-line with adult content. For those investigating CSEM, this may be viewed as a positive, as society has reinforced the need to keep one's computer safe and secure but has been slow

to emphasize the importance of securing one's mobile device. As a result, people are less likely to have protection on their mobile device than their computer and thus provide exploits for law enforcement to identify the user (Alsaleh et al. 2017; McGill and Thompson 2017).

Investigating CSEM

There are three primary goals when conducting investigations of child sexual abuse. The first is to rescue children being abused. The second is to arrest those abusing children. The third is to deter others from engaging in the activity. In general, there are two ways in which online child sexual exploitation is investigated. The first is through nation-sanctioned investigations that may span multiple countries and law enforcement agencies, as well as obtain cooperation/assistance of technology companies and nonprofit organizations. The second is through self-appointed vigilante operations conducted by citizens who believe they are assisting law enforcement and shaming offenders who engage in child sexual exploitation. While nation-sanctioned and vigilante efforts dominate, there have been calls upon Internet service providers to assist with investigating cases.

Nation-Sanctioned Investigations

The vastness of online CSEM production and distribution has led to combat efforts being undertaken by national and international law enforcement agencies, such as the Federal Bureau of Investigations and Interpol; nongovernmental technology organizations, such as Google and Microsoft; and nonprofit organizations, such as the International/National Center for Missing and Exploited Children, CyberTip.ca, and Thorn. Together, they conduct investigations, develop tools, and maintain image and video databases.

In the United States, Internet Crimes Against Children (ICAC) task forces play an important role investigating online child sexual abuse as they are often the ones to receive tips through agencies such as NCMEC and are the tip of the spear for federal investigators. Created in 1998 by the Office of Juvenile Justice and Delinquency Prevention (OJJDP), ICACs are a national network of 61 task forces with the aim of combating child sexual exploitation through investigations, training, education, technical assistance, and victim services (ICAC 2017; OJJDP n.d.). Since 1998 ICACs have reviewed nearly 850,000 complaints and arrested almost 90,000 people. In 2018 alone, ICACs conducted more than 71,200 investigations and 84,700 forensic exams leading to more than 9,100 arrests. Additionally, they trained over 46,500 law enforcement personnel, 2,900 prosecutors, and 14,300 professionals working in the field. ICACs have been funded until at least 2022, with a 2018 budget of $28.6 million.

Because the Internet does not conform to national boundaries, cooperative international operations are pertinent to combating CSEM production and distribution. Central to these operations is the Virtual Global Taskforce (VGT 2016). Comprised of 12 board managers/advisors from North and South America, Europe, Middle East, Asia, and Oceania, and chaired by Canada's Royal Canadian Mounted Police, VGT connects government, nongovernment, and industry partners to combat child sexual exploitation. The belief is that protecting children requires global, rather than just national, efforts and thus assist in pursuing strategic investigations.

In the 1990s, some of the most prominent international operations included Cathedral/Wonderland Club (1998), which involved 12 countries and led to 107 arrests and the identification of 1,236 children, and Avalanche (1999), which involved 60 countries and more than 100 arrests in the United States. In the 2000s, the United Kingdom-based Ore (2002) led to 1,670 people being charged and 1,230 being convicted. Delego (2009) led to the arrest of 52 people in 14 countries and the dismantling of a large, members-only, website named *Dreamboard*, which required members to submit new material every 50 days to maintain their status. More recently, operations have become bigger. Thunderer/Project Spade (2013) involved cooperation between 50 countries and simultaneous arrests of over 350 people, leading to 386 children being rescued. Pacifier (2015) saw the 150,000-user website Playpen get shutdown, in one of the largest and most complicated international operations, leading to at least 870 arrests and the identification or rescue of more than 259 children (Europol 2017). Finally, in 2018, US-based Broken Heart led to the arrest of more than 2,300 suspects, including 195 who produced CSEM or committed sexual abuse of 383 children (Office of Public Affairs 2018).

Vigilante Investigations

Like many other types of crimes, citizens have taken it upon themselves to engage in crime enforcement in cases of online child sexual exploitation, through vigilante justice groups. Many of these groups enter chat rooms and attempt to lure predators into identifying themselves and/or meeting for a sexual encounter. For those that identify themselves, vigilantes disseminate information about the predator's actions to various sources including employers and family members. For those that agree to a sexual encounter, vigilantes have been known to assault predators when they arrive at the specified location. A popular example of vigilante justice was the television show *To Catch a Predator*, which ran from 2004 to 2007. In the show, a person impersonated a teenager and attempted to lure adult men to a location for sexual liaisons. When the men arrived, they were confronted by show host Chris Hansen and then local law enforcement. The show conducted 12 investigations before being canceled, allegedly due to a Texas District Attorney assistant shooting themselves after being caught (Eaton 2006).

To combat child sex tourism, Terre des Hommes (2015) developed "Sweetie," a digital 11-year-old Philippine girl, to interact, identify, and deter predators who

solicit children in chat rooms. In 2015, they introduced Sweetie 2.0, an avatar of various virtual children who uses artificial intelligence to engage with multiple offenders simultaneously. Upon entering a chat room and being contacted, the bot attempts to get predators to (a) admit they know they are conversing with a child, (b) request to see the child without clothes, and (c) offer to pay the child to remove their clothes. Once these three criteria have been met, the bot begins gathering data by having the predator share personal details about themselves such as email addresses and social media accounts. Terre des Hommes takes that information and sends warming messages to the person stating that they know who they are, where they are, and what they are/were attempting to engage in. The group sees this as a form of early intervention to prevent future sexual exploitation of children online and in-person.

Given the substantial amount of CSEM and offenders on the Internet, it is understandable why vigilante justice has become a popular tactic; however, there have been questions raised about how much these groups are actually helping (Perraudin 2017). The action of these people can be counterproductive as they may jeopardize police operations by driving offenders underground or to new locations. Additionally, learning how they were identified may assist abusers with developing more effective techniques for hiding their identities, making police operations more difficult.

Internet Service Providers (ISPs)

As nations and vigilantes conduct investigations of sexual abusers of children, ISPs have sat mostly on the sidelines. Providing an (almost) essential service, and thus needing to be regulated, but also being nongovernment entities, ISPs occupy a unique role within society. As gatekeepers to the Internet, ISPs wield significant power. Yet, governments have been slow to implement responsibilities upon ISPs. A 2016 review of global legislation by ICMEC revealed that only 18 of 196 countries had laws specifically requiring ISPs to report CSEM to law enforcement. In the United States, ISPs are required to inform the NCMEC when they become aware of (a) sexual exploitation of children, (b) production or distribution of CSEM, and (c) websites designed to trick minors into viewing obscene material. In reporting the incident, they must include the email address and/or Internet protocol address of the user, history of transmissions, and geographic area of the individual. However, ISPs are neither required to actively search for CSEM nor monitor for this activity. As a result, the effectiveness, and responsibility, of ISPs in combating the production and dissemination of CSEM is unclear (McCabe 2007).

There have long been calls on ISPs to aid in preventing criminal activity (e.g., copyright infringement); however, arguments have been made that this is impossible as it would require extensive monitoring by ISPs, given the amount of data they process. This is seen as being too labor intensive and financially prohibitive and a potential violation of customer privacy. Moreover, like with hosting services that

are willing to ignore criminal activity, website registration services that mask the identity of website ownership, or virtual private network services that do not keep logs of who uses their services, ISPs would enter the marketplace that refused to monitor user activity. Therefore, it is argued by ISPs that any efforts on their part would be minimally effective in combatting CSEM production and distribution. Still, some is better than none and technology development could improve their effectiveness over time.

Developing Tools to Detect CSEM

Investigating child sexual exploitation and child sexual abuse is difficult due to the lack of cooperation between government bodies, resources, and manpower (Wortley and Smallbone 2012). Research into the experiences of Integrated Child Exploitation (ICE) units has shown that investigators are at increased risks for burnout and psychological harm. Interviewing 32 ICE investigators, Powell et al. (2014) found that large workloads and insufficient time and resources were stressors resulting in burnout. Investigators also suffered from higher rates of secondary traumatic stress disorder, emotional exhaustion, intrusive thoughts, and interpersonal/marriage problems (Bourke and Craun 2014; Burns et al. 2008; Craun et al. 2015; Krause 2009; Perez et al. 2010).

To address some of the challenges investigators face, nongovernment agencies, such as nonprofits, technology companies, and academics, have partnered with law enforcement to develop tools and techniques for identifying CSEM. These partnerships often aim to reduce the amount of contact investigators have with graphic material and to increase the efficiency of detection, in order to maximize the limited resources available. As a result, the tools developed regularly combine CSE-related databases with some form of automated detection of CSEM.

CSEM Databases

One of the simplest methods for identifying CSEM is to search for keywords commonly associated with child sexual abuse or child sexual exploitation. Words such as PTHC (preteen hardcore), Lolita, jailbait, etc. can be searched on public or semipublic P2P networks to find those distributing content. This method has proven useful for researchers, who can use these keywords to study distribution frequencies (Frank et al. 2010; LeGrand et al. 2009; Steel 2009, 2015; Vehovar et al. 2009). However, language is always evolving and thus "popular" keywords are likely to change over time. In addition, as offenders become aware of law enforcement activities, key players within CSEM distribution networks are likely to change their keywords to avoid detection. Therefore, this technique relies on time-consuming searches with many false positives. Nevertheless, some keywords have persisted over time, as new offenders need to find a way to integrate into the community. As 2018s Operation Broken Heart revealed, in which more than half of those arrested

relied on P2P file-sharing programs (The Spokesman-Review 2018), this method of detection can still be mildly effective.

Moving beyond keywords, many law enforcement agencies, such as Interpol, and nonprofit organizations, such as the International Center for Missing and Exploited Children (Project VIC), maintain databases of known CSEM. These databases are primarily comprised of image hash values but are increasingly including video hash values. A hash value is a hexadecimal code which acts like a digital fingerprint for any file. If a file is edited, even slightly, a new hash value is created. The Netherlands Forensic Institute (2018) states that the probability of two files having the same MD5, SHA-1, and/or SHA-256 hash value is, at least, 2.9×10^{-39}. While hash value databases have proven integral to national and international operations, their precision is also their biggest limitation. More specifically, if an offender edits an image or a website resizes an image upon upload, a new hash value is created. As a result, it is easy for multiple hash values to be linked to the same, or very similar, CSEM. Additionally, hash value databases require that the hash already be known. Therefore, databases are not very useful for finding new content.

To address some of the issues with hash value databases, and the challenges of sharing information, technology companies Microsoft and Google have developed some important tools. Working with the Royal Canadian Mounted Police and the Toronto Police Service, Microsoft developed the Child Exploitation Tracking System (CETS). Officially launched on April 7, 2005, CETS aids police agencies in managing and analyzing huge volumes of information in powerful new ways, such as cross-referencing obscure data relationships and using social network analysis to identify communities of offenders (Microsoft 2005). The program allows investigators to easily import, organize, analyze, share, and search information from the point of detection right through the investigative phase.

Integrated into CETS is Microsoft's (2009) PhotoDNA. This program was created to address the limitation of hash values by using fuzzy logic (see Zadeh 2008) to detect modified versions of known hash values. This automated tool aids in the detection process as it allows for the analysis of a large quantity of images in a short period of time. Similarly, Google adapted its pattern recognition software, originally used on YouTube to detect copyrighted material, to aid in organizing and indexing CSEM so analysts can better deal with new images and videos (Baluja 2008). In 2018, Google in Europe announced the introduction of artificial intelligence (deep neural networking) to their image processing software to assist reviewers with prioritizing content most likely to be CSEM. With so much CSEM being distributed online, it is important that tools continue to be developed that increase the automation of detection and the ability to find new content.

As Internet speeds increase, and offenders move away from static media (images) toward dynamic media (videos), the importance of video databases increases. However, video hash values are limited as they can only be used to determine equality or non-equality of data files. Like how PhotoDNA and Google's pattern recognition software have been developed to use image hash values as a starting point, and subsequently find similar images, video fingerprinting can be, and has been, used in the same way for CSE videos. Video fingerprinting is a technique

in which software identifies, extracts, compresses, and summarizes characteristic components of videos, to allow them to be uniquely identified (i.e., fingerprinted). This is useful for comparing digital video data in which difference in codecs and/or digital processing artifacts (e.g., resolution, cropping, and blurring) has led to different hash values, despite the videos being the same. The technique has been used in cases of unauthorized distribution of copyrighted material, and similar techniques have recently been introduced into PhotoDNA (Langston 2018) and likely Google's software too.

For each of the aforementioned techniques, a key requirement is that the CSEM being analyzed has already been categorized within a database. To better assist investigators, tools need to be developed that can identify previously unknown CEM, as well as their distribution pathways. The artificial intelligence announcement by Google signals the beginning of a new wave in how CSEM is identified: the use of voice and facial recognition (biometrics) in automated searches. Biometrics involves analyzing uniquely identifying biological traits to identify specific individuals. One of the oldest forms of biometrics is fingerprint identification.

Voice and facial recognition are not without their challenges. For voice-based biometrics, speaker recognition from degraded audio data can be a major roadblock. However, Mel Frequency Cepstral Coefficients and Linear Predictive Coding can assist in determining speech perception and production. When combined in a novel manner, these can enhance the performance of speaker recognition in challenging scenarios. For face-based biometrics, poor quality data can also be a problem. However, through the design and training of a deep-learning face matcher, faces can be decomposed into multiple semantic components. This would allow for the analysis of a broad spectrum of face images (multiple pose, illumination, expression, age, resolution, etc.). The goal would be to elicit the "identity" component while suppressing the other "noisy" components.

By utilizing biometrics, connections between CSEM found on multiple websites can be made, which may link locations, victims, and/or offenders. Through scanning unknown images and videos and comparing their biometrics to a database of known victims (and offenders), biometrics can aid in determining whether CSEM is new, previously known, or irrelevant. For example, the tool could report that "on Website A, there is a video located at [direct video address] that is an 74% audio match for Victim 184." The investigator would then go directly to the provided web address, examine the media, and determine if it is new, previously known, or an incorrect identification (i.e., false positive). Being able to make these linkages can increase the likelihood of rescuing abused children. For example, if investigators know that two videos, featuring different children, are produced by the same offender or in the same location, pieces of information from each video can be combined to formulate a more accurate profile.

The validation of automated tools and the continued improvement and refinement of features, such as biometrics, can aid in reducing the amount of direct, and continuous, contact investigators need to have with CSEM. While investigators still need to verify the findings of these tools, and examine the identified CSEM,

the reduction in direct contact with CSEM has significant potential to decrease the mental and physical trauma experienced, thereby reducing the health costs associated with investigating this topic. Furthermore, by automating a large portion of the scanning, collecting, and initial analyzing of CSEM, investigators can focus more on the identification and recovery (rescue) of victims from harm.

Understanding How CSEM Is Distributed

The ability to better identify CSEM is important for reactive responses to distribution; however, understanding better how CSEM is initially distributed is equally important for proactive responses to distribution. To do this, there needs to be improved awareness of how new CSEM enters the online market and is initially distributed. Many tools that currently exist require that CSEM be previously known. As a result, investigators know very little about the initial stages of a child sexual exploitation media's life course. For example, does a new image show up on one website and then slowly, or quickly, saturate the network; or does it show up on multiple websites almost immediately? How long before new CSEM saturates the network? Are certain types of CSEM (e.g., videos, stories, images) distributed differently or do they follow the same pattern? Can specific key players/websites be targeted that can greatly reduce production and dissemination? By integrating biometrics identification with social network analyses, investigators can determine how CSEM distribution evolves and develop better strategies for disrupting and dismantling exploitative networks.

Social Network Analysis

Social science research has traditionally explained the behaviors of an individual through their personal characteristics, whether those be primarily psychological or sociological. However, as the debate between peer influence and selection shows (Haynie 2001, 2002), there is acknowledgment that the subsequent behavior of an individual may be influenced as much by their surrounding environmental structure as their personal characteristics. Social network analysis (SNA) involves examining the linkages and interdependence of social interactions between different units (e.g., people) in a bound network to explain behavior (Wasserman and Faust 1994; Wellman 1983). That is, if two groups of equally skilled people are compared, their overall performance will be dependent on the relationships between group members (Borgatti et al. 2009).

SNA is a theoretical and methodological paradigm that can be used to observe and measure the importance of social structures by analyzing the relationships between nodes (e.g., people, organizations, and websites) and connections (Borgatti and Halgin 2011; Papachristos 2011). These relationships can be positive or negative and can influence the behavior of the individual nodes and/or the surrounding network. Borgatti et al. (2009) summarize relationships (i.e., ties) into four

types: (1) similarities (e.g., location, membership, or attribute), (2) social relationships (e.g., kinship, affective, or cognitive), (3) personal interactions, and (4) flows (e.g., information, beliefs, resources, or personnel). As a theoretical paradigm, SNA is characterized by three theoretical concepts (Borgatti et al. 2009): (1) the shape and cohesion of the network structure, measured through network density, the clustering coefficient, and fragmentation; (2) the position of nodes within the network, measured through centrality, degree, closeness, and betweenness; and (3) the dyadic cohesion and equivalence, referring to the social closeness (dyadic cohesion) and the similarity in network roles (equivalence) of any pair of nodes.

The nature of online interactions and digital information makes the Internet an ideal location for applying SNA. Online interactions are inherently social network based. Between people, this is conducted through direct communications between a sender and a receiver. Between websites, social networks are created through hyperlinked webpages. The nature of digital information also makes it conducive to SNA as network data are not dependent on in-person data collection, perception, or memory. Rather, there is concrete evidence of connectivity frequency and importance that is easy to measure. This means that the presence of a relationship (tie) and the strength of that relationship can be quantified through straightforward methods.

The importance of SNA in the study of online child sexual abuse has also been acknowledged most notably by Krone (2004), who stated that the linkages between distributors may be as important to understanding the phenomenon as the material that is being distributed. Following Krone's statement, SNA has been used to identify the network structure (Frank et al. 2010), cliques (Iqbal et al. 2012), communities (Westlake and Bouchard 2016a), key players (Westlake et al. 2011; Westlake and Frank 2017), optimal strategies for network disruption (Allsup et al. 2015; Joffres et al. 2011), and traits of website survival (Westlake and Bouchard 2016b) within the study of online child sexual abuse.

Network Capital: Identifying Key Websites/Players

Combining a tool developed to automatically identify CSEM with SNA target prioritization techniques, Westlake et al. (2011) adapted Schwartz and Rouselle's (2009) measurement of *network capital* to the specific context of online child sexual exploitation networks. Built upon the foundation of Borgatti's (2006) method for identifying key players, Westlake and colleagues' original network capital measurement took into consideration the resources available to each website (node), the cohesiveness of the overall network, and the relationship between the nodes. This was accomplished by calculating two components. First was the amount of CSEM made available (resources) and the hyperlinks to other websites within the network (connectivity).

The original network capital measurement was limited in scope as it did not consider two underlying attributes central to combat. First, disrupting CEM distribution is complicated by jurisdictional boundaries. As such, target prioritization strategies need to consider the physical location of the material and the offender.

Second, some websites are operated by the same individual or groups of people. As such, we would expect to see higher rates of connectivity and overlap in content between these websites. This overlap would impact network capital and by association target prioritization. For example, if five websites were operated by the same owner, then all five would need to be shutdown at once as the removal of only one would result in minimal impact on CSEM distribution within the network. Likewise, if those five websites were smaller, but operated by the same person, their targeting could have a greater impact on distribution than the targeting of a larger, singular, website.

In a follow-up to their original work, Westlake and Frank (2017) increased the number of resources included to five and the number of connectivity measures to two. More importantly, they incorporated geolocation of the domain hosting the website, the image hosting service, and the Whois registrant information. This aided in identifying jurisdiction as well as connections between multiple websites (e.g., being operated by the same person/organization). In this research, Westlake and Frank first showed the effectiveness of strategic target prioritization based on network capital and its components (Table 2). When compared to the overall "scores" for the network on resources, connectivity, and network capital, the removal of the top three websites on each measure led to a greater reduction in the overall network capital score (7%), and the corresponding resource and connectivity scores, than when three websites were chosen at random and removed from the network (4%). Second, Westlake and Frank showed that while targeting the websites with the highest network capital scores is useful, jurisdictional issues can impede this strategy. Figure 2 visualizes a network of 83 websites and identifies the nation location of each. Although eight of the ten highest network capital score websites were in the United States, two were in the Netherlands. This finding emphasized the importance of international cooperation and information sharing. Third, Westlake and Frank revealed that website ownership can be an even more important component of target strategizing. In Fig. 3, Owner #1 operates the six websites on the far right, while Owner #2 operates the four websites on the center bottom. While none of the

Table 2 Change in network capital when removing three websites using targeted (top contributors) and non-targeted (random) strategies

	Resources	Connectivity	Network capital (NC)	Δ in NC[a]
Original	16.42	38.86	8.03	–
Top 3 resources	14.67	37.04	7.51	6.93%
Top 3 connections	15.04	36.67	7.51	6.91%
Top 3 network capital	14.76	36.83	7.49	7.16%
Random 1	15.78	37.27	7.70	4.22%
Random 2	15.78	37.15	7.68	4.47%
Random 3	15.76	37.19	7.69	4.43%
Random 4	16.02	37.75	7.81	2.82%
Random 5	15.57	37.04	7.64	5.09%

Source: Westlake and Frank (2017)
[a]Discrepancy due to rounding

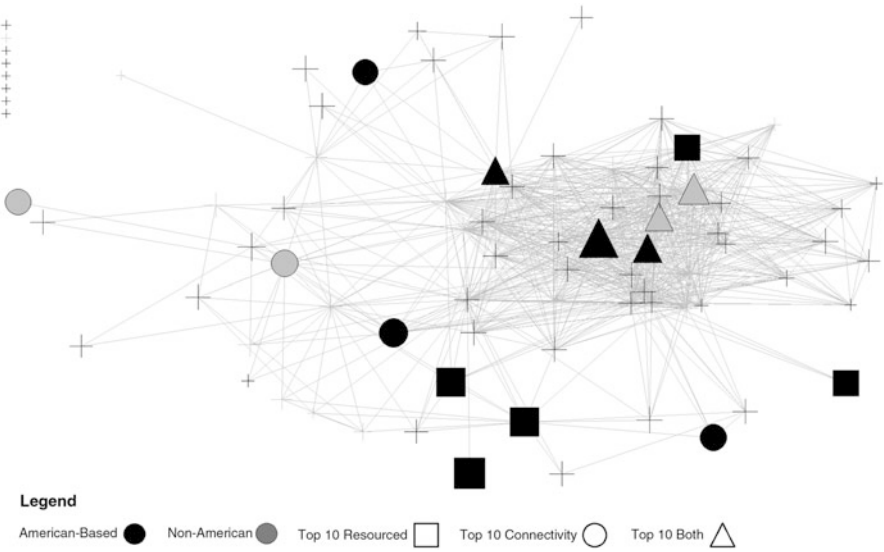

Fig. 2 The top ten most resource-rich or connected child sexual exploitation websites and those that are top ten in both. (Source: Westlake and Frank (2017))

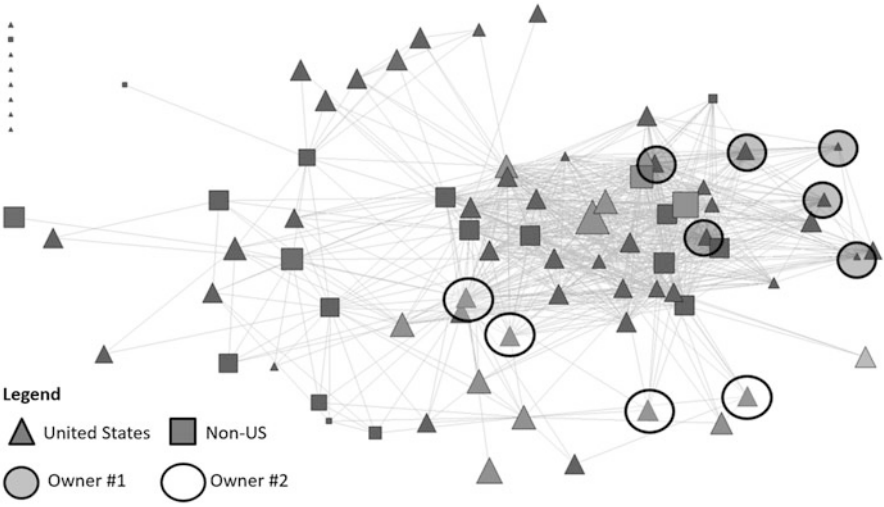

Fig. 3 Website hosting country with two prominent website owners highlighted

websites are identified as being among the highest in resources or connectivity, the removal of Owner #1 leads to a 5.17% reduction in overall network capital, whereas the removal of Owner #2 leads to a 5.95% reduction. Therefore, by

targeting specific owners in addition to those with a lot of CSEM or connectivity, limited law enforcement resources can be maximized.

The validation of automated data collection tools and the continued improvement and refinement to their criteria reliability, features, and overall performance can aid in reducing investigator health costs. By automating the scanning and data collection process, officers can spend more time investigating cases rather than searching the Internet for material. Through automation, officers would also view less material for verification purposes and be able to focus website searches on, for example, previously catalogued material. In addition, automated tools can be deployed on the Internet, in general, or on individual websites on the Surface and Deep/Dark Web by website owners or law enforcement agencies. This approach can be useful as the Internet community – large technology companies – would play a critical role in reducing the amount of CSEM being distributed through their services and decrease the amount of material investigators need to analyze. Integrating biometrics into these automated tools can further improve detection as new CSEM can be identified quicker, decreasing the time to the rescuing of children offline. Combined with social network analyses, the data collected can be used to improve prioritization strategies by finding key players/targets rather than blindly swinging at websites and better understanding the evolution of CSEM as it enters the online marketplace.

Growing Trends in CSEM

Like with all forms of cybercrime, technological advancements continue to change the online child sexual exploitation landscape. While efforts to date to combat CSEM production and distribution have focused on adults, there has been a recent trend whereby youth are developing and disseminating their own material. Additionally, attempts to make adult pornography more immersive and interactive have led to a boom in virtual reality's presence and applicability, while the global reach of the Internet has allowed those within long-distance relationships to engage in sexual intimacy through teledildonics: technology that can be used to remotely control dildos (typically phallic-shaped insertable objects used for sexual stimulation) through their attachment to a computer via a usb slot.

Although there is no evidence that virtual reality and teledildonics have become prominent within online child sexual exploitation, there is no reason to believe that they will not follow the adult trends and become common problems in newly produced videos (virtual reality) and webcam/chat room exploitation (teledildonics), especially in the realm of self-produced material.

Self-Produced CSEM

A Pew Internet survey revealed that 76% of 15- to 17-year-olds owned a smartphone, with 92% of teenagers aged 13–17 reporting daily Internet use and

24% reporting "almost constant" use (Lenhart 2015). This degree of cellular phone ownership among adolescence, capable of taking high-resolution images, has led to a significant increase in rates of sexting. However, cellular phones are not the only medium in which self-produced CSEM is appearing. Examining criminal cases of teenage sexting, Wolak et al. (2012) found that while 78% involved the use of a cellular phone, 41% involved the use of a computer or online website. In 2006, NCMEC found that 6% of CSEM on the Internet was self-produced. By 2014, that number had risen to 14% (Sparks 2016).

Although some self-produced content is being redistributed by adults, a growing number of teenagers are engaging in live, webcam-based, self-exploitation, and distributing the content on their personal websites. For adolescents who participate in this practice, there are opportunities for monetary gain, gifts from fans, and admiration that they might not otherwise receive (Bocij 2004; Jonsson et al. 2015). One highly publicized case was that of Justin Berry (Eichenwald 2005; Soderlund 2008). Beginning at the age of 13, Berry operated a webcam from his bedroom, performing sexual acts in exchange for gifts and money from adult fans. Justin's first venture into online SPCP was when he was offered $50 in a chat room in exchange for baring his chest to the webcam for 3 min. Seeing no harm in the act, and being acutely aware of the financial gain available, he agreed to the request. Berry's acts escalated to include sex with prostitutes and with other teenagers he recruited to join his online business.

To better understand the demographics of those engaging in self-produced CSEM, IWF (2015; 2018) conducted two studies (Table 3). The first was in 2014 and consisted of 3,803 cases. The second was in 2017 and consisted of 2,082 cases. Like with adult-produced CSEM, the content was largely of girls; however, it was less likely to involve explicit and/or extreme sexual acts and comprised of older children. Nevertheless, in the 2014 study, nearly 43% of material was of children under the age of 11, while in the 2017 study, it was slightly more than 28%.

Different from webcam child sex tourism (WCST), which involves adults paying to observe and direct children in sexually explicit activities (Puffer et al. 2014), self-produced CSEM from "non-coerced" teenagers create a complication for enforcement agencies and judicial systems. Countries have begun to develop laws to

Table 3 Two IWF studies on demographics of self-produced CSEM

Timeframe		2014	2017
Number of cases		3,803	2,082
Age of victim(s)	Toddlers	2.50%	0.10%
	Under 11	40.30%	28.10%
	Over 11	57.10%	71.76%
Sex of victim(s)	Boys	7.05%	3.12%
	Girls	94.45%	98.13%
Content severity	Sexual posing	53.10%	60.18%
	Extreme posing	44.80%	21.95%
	Explicit/extreme sex acts	2.10%	17.87%

delineate self-produced content and adult-produced CSEM; however, these laws have almost entirely focused on sexting between two consenting teenagers (e.g., Bosak 2012; Duncan 2010). Omitted from many, if not all, of these law revisions are instances where teenagers profit from their own exploitation, akin to self-child prostitution (Adelson 2008). A likely reason for this is that lawmakers have not considered that a child would do this. Additionally, developing laws for these types of scenarios is complex as the youth can be viewed as both an offender and a victim (Westlake 2018).

Virtual Reality and Teledildonics

Another growing trend within online pornography is the emergence of virtual reality. From June 2016 to January 2017, Pornhub saw an increase in daily views of virtual reality pornography rise from 200,000 to 500,000 (Pornhub Insights 2017). When examining where adult virtual reality pornography is most popular, Pornhub found that Thailand, Philippines, and Taiwan were among the top five; all with a history of being hotbeds for WCST. Today, the most commonly searched term linked to virtual reality is "porn," with more than 60% of the top 50 virtual reality websites being dedicated to pornography, including the first-, third-, and fourth-most visited websites (VRPorn.com 2017).

There is no evidence that virtual reality has made inroads into CSEM; however, it is likely that virtual reality may prove to be the next challenge society faces in combating CSEM. Of course, one of the advantages of virtual reality for law enforcement agencies is that the immersive environment can mean that investigators are able to examine the environment in which the abuse is occurring more closely and find clues that can lead to an arrest and the rescuing of a child. However, this also means placing investigators in somewhat realistic, first-person, viewpoints of child sexual abuse. As a result, this may lead to even higher rates of psychological harm and burnout.

Finally, growth in adult camming – performing sexual services, via live webcam, in exchange for money, goods, and/or attention – has led to advancements in sexual intimacy aids. For adult camming, teledildonics allows customers to interact with the model and control the sexual activity/pleasure experienced. Customers submit a monetary value, determined by the model, and that monetary value changes the movement and/or intensity of the toy. Like with virtual reality, there is no evidence that teledildonics has appeared within CSEM. However, the movement in both adult-directed and self-produced CSEM to video and live streaming suggest that, like virtual reality, teledildonics will be a common practice within CSEM. When/if this occurs, it will create challenges for law enforcement and prosecutors as some countries require physical penetration for an offender to be charged with rape. Furthermore, it will further fuel the discussion over the criminalization of virtual sexual assault (Danaher 2018; Dibbell 1993). Where this is most likely to be seen first is in self-produced material and WCST.

Growth in sexting and self-produced CSEM, along with the possibility/reality of virtual reality and teledildonics, should not be viewed independently from one another. Instead, these new-age sex crimes, conducted in cyberspace, need to be examined and addressed together. However, like with adult-directed CSEM, the examination needs to consider all possibilities and to help us better understand how each type of crime manifests independently and/or in conjunction with others. Through an examination of the broader problem, appropriate strategies can be developed.

Avenues for Future Research

Over the last 20 years, rates, or at least visibility, of child sexual exploitation have risen sharply, thanks to the global reach and accessibility of the Internet. As the Internet expands, access becomes faster and laws continue to lag behind, and as offenders increase in confidence and minimize risk through methods of anonymity, it will become increasingly difficult to effectively combat CSEM distribution. There is reason to believe that the problem will continue to grow, with unanticipated trends arising among youth as they take their sexual expression into their own hands and engage willingly or coercively in self-exploitation online. As society is unable to effectively contain CSEM distribution, our study of the problem needs to see a shift in focus.

In general, one of the challenges that all scientists face is taking what they have found and applying it beyond the laboratory setting. Within the study of online child sexual exploitation, and child sexual abuse, research has focused heavily on what is CSEM and the techniques used to distribute CSEM. However, when you speak with investigators, there is little that is currently studied by academics that is not already common knowledge within the field. A lot of our understanding of CSEM online is through retroactive examination. More accurately, it relies heavily on examining CSEM that is already known to investigators and is heavily circulated. As a result, it does little to curb the problem and little to assist law enforcement outside of the laboratory setting. This is because identifying and removing a website that is distributing CSEM that is several years old, and already known, does little to help the here and now. Therefore, future research instead needs to shift focus to getting ahead of the problem by developing ways to identify previously unknown CSEM (e.g., through biometrics) and understanding how that *new* content is disseminated online (e.g., through social network analysis). This is because the focus of law enforcement is not on how CSEM from 5 years ago is distributed but rather how they can rescue a child being victimized today.

A key component of developing methods for identifying new CSEM and understanding how it enters the online marketplace is interdisciplinary collaboration. While the most obvious partnership is between social scientists and computer scientists/engineers, there also needs to be collaboration between law enforcement, nongovernment agencies, and academics. We have begun to see increased communication between investigators and industry; however, it is still not enough. In many

countries only law enforcement can legally possess CSEM. While this is understandable, it handcuffs the ability of scientists to make meaningful contributions to combating CSEM production and distribution. Therefore, it is important that law enforcement reaches out to academics and develops partnerships outlining what tools and information would be most useful for their investigations and provides researchers with the resources to design and validate those techniques. This does not necessarily mean giving non-investigators access to CSEM. However, it does mean working with researchers to describe what information they have about CSEM and be willing to test out techniques designed by interdisciplinary collaboration on CSEM databases and investigations.

Studies of online CSEM have relied heavily on the examination of websites and P2P networks. While these are useful, there is little study of emerging methods. For example, within copyright infringement (i.e., piracy), advancements in accessibility to cloud technology and shared drives (e.g., Google Drive and One Drive) have led to offenders distributing new content through these more private methods rather than through publicly accessible websites and P2P networks (Wang 2017). It is likely that these techniques are being used by CSEM producers and disseminators. Meanwhile, the use of virtual reality and teledildonics in adult pornography suggests that it may come to child sexual exploitation at some point soon. Yet, there is currently no literature examining these emerging methods or even discussing how best to address them. While it is complicated, there needs to be a shift in scholarly work to a more proactive and "today" mentality rather than a reactive and "yesterday" mentality.

Part of the reason for the gap between offenders using a technology and researchers studying its use is that many are unaware or only mildly aware of these new methods. This is evidenced through the slow reaction by lawmakers and researchers to the quick growth of teenage sexting. As teenage sexting has become a hot topic in society and research, there remains very little focused on self-exploitation (Westlake 2018). Again, this is evidence of the reactionary way of conducting research and developing policies. This is not necessarily the fault of anyone, but rather reinforces the importance of open communication and collaboration between investigators and non-investigators, to ensure that what scholars are studying, what technology companies are building, and what policies are being discussed by government officials is relevant to what we are seeing in today's landscape.

Conclusion

The production, distribution, and consumption of CSEM in cyberspace continue to be a problem with no signs of slowing down. In fact, with advancements in technology and access to additional platforms to produce and disseminate CSEM growing, the problem is likely to get worse as we move forward. As global law enforcement agencies and nongovernment entities come together, advancements are being made to reduce access to CSEM and trauma experienced by those willing to investigate child sexual abuse on a daily basis. As technology utilized in other

domains, such as biometrics, is introduced into the fight against online child sexual exploitation, there are reasons to be optimistic that inroads can be made. If these innovations are combined with analysis techniques such as social network analysis, it is possible that those combating child sexual abuse can improve their methods and get ahead of mass distribution by accurately predicting future patterns. However, society must remain vigilant and work together to address this issue. In addition, pressure needs to be placed on governments and Internet service providers to be proactive with enforcement and provide the judicial and data tools necessary to combat CSEM distribution.

References

Adelson, W. J. (2008). Child prostitute or victim of trafficking. *University of St. Thomas Law Journal, 6*(1), 96–128.

Allsup, R., Thomas, E., Monk, B., Frank, R., & Bouchard, M. (August 2015). Networking in child exploitation: Assessing disruption strategies using registrant information. In *Proceedings of the 2015 IEEE/ACM international conference on advances in social network analysis and mining 2015* (pp. 400–407). Paris, France: ACM.

Alsaleh, M., Alomar, N., & Alarifi, A. (2017). Smartphone users: Understanding how security mechanisms are perceived and new persuasive methods. *PLoS One, 12*(3), e0173284. https://doi.org/10.1371/journal.pone.0173284.

Baluja, S. (2008, April 14). *Building software tools to find child victims*. Retrieved from http://googleblog.blogspot.com/2008/04/building-software-tools-to-find-child.html

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.

Bocii, P. (2004). Camgirls, blogs and wish lists: How young people are courting danger on the internet. *Safer Communities, 3*(3), 16–22. https://doi.org/10.1108/17578043200400018.

Borgatti, S. (2006). Identifying sets of key players in a social network. *Computational & Mathematical Organization Theory, 12*(1), 21–34.

Borgatti, S. P., & Halgin, D. S. (2011). On network theory. *Organization Science, 22*(5), 1168–1181. https://doi.org/10.1287/orsc.1100.0641.

Borgatti, S. P., Mehra, A., Brass, D. J., & Labianca, G. (2009). Network analysis in the social sciences. *Science, 323*(5916), 892–895. https://doi.org/10.1126/science.1165821.

Bosak, D. (2012). The blurring line between victim and offender: Self-produced child pornography and the need for sentencing reform. *Ohio State Law Journal, 73*, 141–176.

Bourke, M. L., & Craun, S. W. (2014). Secondary traumatic stress among internet crimes against children task force personnel. *Sexual Abuse: A Journal of Research and Treatment, 26*(6), 586–609. https://doi.org/10.1177/1079063213509411.

Bullough, V. L. (2004). Children and adolescents as sexual beings: A historical overview. *Child and Adolescent Psychiatric Clinics of North America, 13*(3), 447–459.

Burgess, A. W. (1984). *Child pornography and sex rings*. New York: Lexington Books.

Burns, C. M., Morley, J., Bradshaw, R., & Domene, J. (2008). The emotional impact on coping strategies employed by police teams investigating internet child exploitation. *Traumatology, 14*, 20–31.

Canadian Centre for Child Protection. (2016, January). *Child sexual abuse images on the Internet: A cybertip.ca analysis.* Retrieved from https://www.cybertip.ca/app/en/projects-research

Carr, A. (2004). *Internet traders of child pornography and other censorship offenders in New Zealand*. Wellington: Department of Internal Affairs. Retrieved from http://www.dia.govt.nz/Pubforms.nsf/URL/entirereport.pdf.

Council of Europe (2017, October 25). *Council of Europe convention on the protection of children against sexual exploitation and sexual abuse.* Retrieved from https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/201

Craun, S. W., Bourke, M. L., & Coulson, F. N. (2015). The impact of internet crimes against children work on relationships with families and friends: An exploratory study. *Journal of Family Violence, 30*, 393–402.

Criminal Code, R.S.C. 1985, c.46, s.163.1

Danaher, J. (2018). The law and ethics of virtual sexual assault. In W. Barfield & M. Blitz (Eds.), *Research handbook on the law of virtual and augmented reality* (pp. 363–388). Cheltenham: Edward Elgar Publishers.

Dibbell, J. (1993, December 23). A rape in cyberspace or how an evil clown, a Haitian trickster spirit, two wizards, and a cast of dozens turned a database into a society. *The Village Voice.* Retrieved from https://www.villagevoice.com/2005/10/18/a-rape-in-cyberspace/

Duncan, S. H. (2010). A legal response is necessary for self-produced child pornography: A legislator's checklist for drafting the bill. *Oregon Law Review, 89*, 645–700.

Eaton, T. (2006, November 7). Prosecutor kills himself in Texas raid over child sex. *The New York Times.* Retrieved from https://www.nytimes.com/2006/11/07/us/07pedophile.html

Eichenwald, K. (2005, December 19). Through his webcam, a boy joins a sordid online world. *The New York Times*. Retrieved from http://www.nytimes.com/2005/12/19/us/through-his-webcam-a-boy-joins-a-sordid-online-world.html

Europol. (2017, May 6). *Major online child sexual abuse operation leads to 368 arrests in Europe: Press release.* Retrieved from https://www.europol.europa.eu/newsroom/news/major-online-child-sexual-abuse-operation-leads-to-368-arrests-in-europe

Fournier, R., Cholez, T., Latapy, M., Chrisment, I., Magnien, C., Festor, O., & Daniloff, I. (2014). Comparing pedophile activity in different P2P systems. *Social Sciences, 3*, 314–325.

Frank, R., Westlake, B. G., & Bouchard, M. (2010). The structure and content of online child exploitation. In *Proceedings of the 16th ACM SIGKDD workshop on Intelligence and Security Informatics (ISI-KDD 2010)*., Article 3. Washington, DC: ACM. https://doi.org/10.1145/1938606.1938609.

Google in Europe. (2018, September 3). *Using AI to help organizations detect and report child sexual abuse material online*. Retrieved from https://www.blog.google/around-the-globe/google-europe/using-ai-help-organizations-detect-and-report-child-sexual-abuse-material-online

Haynie, D. L. (2001). Delinquent peers revisited: Does network structure matter? *American Journal of Sociology, 106*, 1013–1057.

Haynie, D. L. (2002). Friendship networks and delinquency: The relative nature of peer delinquency. *Journal of Quantitative Criminology, 18*, 99–134.

Hinduja, S., & Patchin, J. W. (2018, November). *State sexting laws.* Cyberbullying Research Center. Retrieved from https://cyberbullying.org/sexting-laws

ICAC. (2017). ICAC task force program. Retrieved from https://www.icactaskforce.org/about-us

International Center for Missing & Exploited Children. (2016). *Child pornography: Model legislation & global review* (8th ed.). Alexandria: International Center for Missing & Exploited Children.

Internet Watch Foundation. (2015, March 10). *Emerging patterns and trends report #1 online-produced sexual content.* Retrieved from https://www.iwf.org.uk/sites/default/files/inline-files/Online-produced_sexual_content_report_100315.pdf

Internet Watch Foundation. (2016). *IWF annual report 2016*. Retrieved from https://www.iwf.org.uk/report/2016-annual-report

Internet Watch Foundation. (2017). *Annual report 2017*. Retrieved from https://annualreport.iwf.org.uk/pdf/IWF_2017_Annual_Report.pdf

Internet Watch Foundation. (2018). *Trends in online child sexual exploitation: Examining the distribution of captures of live-streamed child sexual abuse*. Cambridgeshire: Internet Watch Foundation.

Iqbal, F., Fung, B. C. M., & Debbabi, M. (2012). Mining criminal networks from chat log. In *2012 IEEE/WIC/ACM International conferences on web intelligence and intelligent agent technology-volume 1* (pp. 332–337). https://doi.org/10.1109/WI-IAT.2012.68.

Jenkins, P. (2001). *Beyond tolerance: Child pornography on the internet*. New York: New York University Press.

Joffres, K., Bouchard, M., Frank, R., & Westlake, B. G. (2011). Strategies to disrupt online child pornography networks. In *Proceedings of the EISIC – European Intelligence and Security Informatics* (pp. 163–170). Athens: IEEE.

Jonsson, L., Svedin, C., & Hyden, M. (2015). Without the internet, I never would have sold sex: Young women selling sex online. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 8*(1), 4. https://doi.org/10.5817/CP2014-1-4.

Krause, M. (2009). Identifying and managing stress in child pornography and child exploitation investigators. *Journal of Police and Criminal Psychology, 24*, 22–29.

Krone, T. (2004). A typology of online child pornography offending. *Trends and Issues in Crime and Criminal Justice, 279*, 1–6.

Langston, J. (2018). *How PhotoDNA for video is being used to fight online child exploitation.* Retrieved from https://news.microsoft.com/on-the-issues/2018/09/12/how-photodna-for-video-is-being-used-to-fight-online-child-exploitation/

LeGrand, B., Guillaume, J., Latapy, M., & Magnien, C. (2009). Technical report on dynamics of paedophile keywords in eDonkey queries. Measurement and analysis of P2P activity against paedophile content project. Retrieved from http://antipaedo.lib6.fr/

Lenhart (2015). A majority of American teens report access to a computer, game console, smartphone and a tablet. Retrieved from: http://www.pewinternet.org/2015/04/09/a-majority-of-american-teens-report-access-to-a-computer-game-console-smartphone-and-a-tablet.

McCabe, K. A. (2007). The role of internet service providers in cases of child pornography and child prostitution. *Social Science Computer Review, 26*(2), 247–251. https://doi.org/10.1177/0894439307301438.

McGill, T., & Thompson, N. (2017). Old risks, new challenges: Exploring differences in security between home computer and mobile device use. *Behaviour & Information Technology, 36*(11), 1111–1124. https://doi.org/10.1080/0144929X.2017.1352028.

Microsoft. (2005, April 7). *Tool thwarts online child predators*. Retrieved from http://www.microsoft.com/presspass/features/2005/apr05/04-07CETS.mspx

Microsoft. (2009, December 15). *New technology fights child porn by tracking its "PhotoDNA"*. Retrieved from https://www.microsoft.com/presspass/features/2009/dec09/12-15photodna.mspx

Missing Kids. (2018). *Child sexual abuse material.* Retrieved from http://www.missingkids.com/theissues/sexualabusematerials

Netherlands Forensic Institute. (2018). *Technical supplement: Forensic use of hash values and associated hash algorithms*. The Hague: Ministry of Justice and Security.

O'Halloran, E., & Quayle, E. (2010). A content analysis of a 'boy love' support forum: Revisiting Durkin and Bryant. *Journal of Sexual Aggression, 16*, 71–85.

Office of Juvenile Justice and Delinquency Prevention. (n.d.). Program summary. Retrieved from https://www.ojjdp.gov/programs/progsummary.asp?pi=3

Office of Public Affairs. (2018, June 12). *More than 2,300 suspected online child sex offenders arrested during operation "Broken Heart": Justice News.* Department of Justice. Retrieved from https://www.justice.gov/opa/pr/more-2300-suspected-online-child-sex-offenders-arrested-during-operation-broken-heart

Papachristos, A. V. (2011). The coming of a networked criminology. *Measuring Crime & Criminality: Advances in Criminological Theory, 17*, 101–140.

Perez, L. M., Jones, J., Englert, D. R., & Sachau, D. (2010). Secondary traumatic stress and burnout among law enforcement investigators exposed to disturbing media images. *Journal of Police and Criminal Psychology, 25*, 113–124.

Perraudin, F. (2017, April 24). *Paedophile hunters jeopardizing police work, says senior officer*. Retrieved from https://www.theguardian.com/society/2017/apr/24/paedophile-hunters-jeopardising-police-work-child-protection

Pornhub Insights (2017, May 11). *Virtual reality porn.* Retrieved from https://www.pornhub.com/insights/virtual-reality

Powell, M., Cassematis, P., Benson, M., Smallbone, S., & Wortley, R. (2014). Police officers' perceptions of their reactions to viewing internet child exploitation material. *Journal of Police and Criminal Psychology, 37*(3), 543–557. https://doi.org/10.1007/s11896-014-9148-z.

Puffer, E., McDonald, K., Pross, M., & Hudson, D. (2014). Webcam child sex tourism: An emerging global issue. *The Research and Scholarship Symposium*, paper 15. Retrieved from http://digitalcommons.cedarville.edu/research_scholarship_symposium/2014/podium_presentations/15

R v Sharpe, S.C.C. 2. (2001).

Rutgaizer, M., Shavitt, Y., Vertman, O., & Zilberman, N. (2012). Detecting pedophile activity in BitTorrent networks. *Lecture Notes in Computer Science, 7192*, 106–115.

Schwartz, D. M., & Rouselle, T. (2009). Using social network analysis to target criminal networks. *Trends in Organized Crime, 12*, 188–207.

Seto, M. C., Buckman, C., Dwyer, R. G., & Quayle, E. (2018). *Production and active trading of child sexual exploitation images depicting identified victims: NCMEC/thorn research report*. Alexandria: Seto.

Soderlund, G. (2008). Journalist or panderer? Framing underage webcam sites. *Sexuality Research & Social Policy, 5*, 62–72.

Sparks A. (2016). Spotlight on sexual exploitation. *Presentation given to Texas children's commission.* Retrieved from http://texaschildrenscommission.gov/media/53063/NCMEC-presentation-for-Childrens-Commission.pdf

Steel, C. M. (2009). Child pornography in peer-to-peer networks. *Child Abuse & Neglect, 33*, 560–568.

Steel, C. M. (2015). Web-based child pornography: The global impact of deterrence efforts and its consumption on mobile platforms. *Child Abuse & Neglect, 44*, 150–158. https://doi.org/10.1016/j.chiabu.2014.12.009.

Technopedia. (2018). *Cyberlocker: What does cyberlocker mean?* Retrieved from https://www.techopedia.com/definition/27694/cyberlocker

Terre des Hommes. (2015, February 27). *Sweetie 2.0: Webcamseks met kinderen de wereld uit.* Retrieved from https://www.terredeshommes.nl/programmas/sweetie-20-webcamseks-met-kinderen-de-wereld-uit

The Spokesman-Review. (2018, June 13). *More than 2,300 people arrested for child porn, sexual abuse in nationwide 'Operation broken heart'.* Retrieved from http://www.spokesman.com/stories/2018/jun/13/more-than-2300-people-arrested-for-child-porn-sexu/

Tremblay, P. (2006). Convergence settings for nonpredatory 'Boy lovers'. In R. Wortley & S. Smallbone (Eds.), *Situational prevention of child sexual abuse* (pp. 145–168). Monsey: Criminal Justice Press.

United Nations. (2002). *Optional protocol to the convention on the rights of the child on the sale of children, child prostitution and child pornography.* Retrieved from https://treaties.un.org/pages/ViewDetails.aspx?src=IND&mtdsg_no=IV-11-c&chapter=4&lang=en

Vehovar, V., Ziberna, A., Kovacic, M., Mrvar, A., & Dousak, M. (2009). Technical report on an empirical investigation of Paedophile keywords in eDonkey P2P network. Measurement and analysis of P2P activity against paedophile content project. Retrieved from http://antipaedo.lib6.fr/

Virtual Global Taskforce. (2016). What is the VGT. Retrieved from https://virtualglobaltaskforce.com/about/vgt-structure

VRPorn.com. (2017). *VR porn and the web: A statistical study.* Retrieved from https://vrporn.com/vr-porn-and-the-web-a-statistical-study/

Wang, S. (2017). The cloud, online piracy and global copyright governance. *International Journal of Cultural Studies, 20*(3), 270–286. https://doi.org/10.1177/1367877916628239.

Waqas. (2018, November 19). *6500 sites down after hackers wipe out database of dark web hosting firm*. Retrieved from https://www.hackread.com/hackers-wipe-out-database-of-dark-web-hosting-firm

Wasserman, S., & Faust, K. (1994). *Social network analysis: Methods and applications*. Cambridge, UK: Cambridge University Press.

Wellman, B. (1983). Network analysis: Some basic principles. *Sociological Theory, 1*, 155–200.

Westlake, B. G. (2018). Delineating victims from perpetrators: Prosecuting self-produced child pornography in youth criminal justice systems. *International Journal of Cyber Criminology, 12*(1), 255–268. https://doi.org/10.5281/zenodo.1467907.

Westlake, B. G., & Bouchard, M. (2016a). Liking and hyperlinking: Examining reciprocity and diversity in online child exploitation network communities. *Social Science Research, 59*, 23–36. https://doi.org/10.1016/j.ssresearch.2016.04.010.

Westlake, B. G., & Bouchard, M. (2016b). Criminal careers in cyberspace: Examining website failure within child exploitation networks. *Justice Quarterly, 33*(7), 1154–1181. https://doi.org/10.1080/07418825.2015.1046393.

Westlake, B. G., & Frank, R. (2017). Seeing the forest through the trees: Identifying key players in online child sexual exploitation distribution networks. In T. Holt (Ed.), *Cybercrime through an interdisciplinary lens* (pp. 189–209). New York: Routledge.

Westlake, B. G., Bouchard, M., & Frank, R. (2011). Finding the key players in online child exploitation networks. *Policy and Internet, 3*(2), 6. https://doi.org/10.2202/1944-2866.1126.

Westlake, B. G., Bouchard, M., & Girodat, A. (2017). How obvious is it: The content of child sexual exploitation websites. *Deviant Behavior, 38*(3), 282–293. https://doi.org/10.1080/01639625.2016.1197001.

Wolak, J., Finkelhor, D., & Mitchell, K. J. (2012). *Trends in law enforcement responses to technology-facilitated child sexual exploitation crimes: The third National Juvenile Online Victimization Study (NJOV-3)*. Durham: Crimes against Children Research Center.

Wolak, J., Liberatore, M., & Levine, B. N. (2014). Measuring a year of child pornography trafficking by U.S. computers on a peer-to-peer network. *Child Abuse & Neglect, 38*(2), 347–356. https://doi.org/10.1016/j.chiabu.2013.10.018.

Wortley, R. K., & Smallbone, S. (2012). *Internet child pornography: Causes, investigation, and prevention*. Santa Barbara: ABC-CLIO.

Zadeh, L. A. (2008). Is there a need for fuzzy logic? *Information Sciences, 178*(13), 2751–2779. https://doi.org/10.1016/j.ins.2008.02.012.