

Child Sex Abuse Images and Exploitation Materials

Roderic Broadhurst

Australian National University Cybercrime Observatory

Rutger Leukfeldt & Thomas Holt, Eds. *Cybercrime: the human factor*, Routledge, forthcoming July 2019

Corresponding address: roderic.broadhurst@anu.edu.au, ANU, School of Global Governance and Regulation.

I am grateful for the assistance of Brigitte Bouhours, Peter Grabosky, Shanmuk Kandukuri, Katrina Pinn and the anonymous reviewers in the preparation of this chapter.

Roderic Broadhurst

ORCID ID

orcid.org/0000-0001-5432-1350

Abstract

Online markets for child exploitation materials (CEM) or child sex abuse images have developed in tandem with the rapid expansion of the Internet. CEM images of sexual abuse of children, often photographs and videos, include live transmission of sexual assault as well as simulated experiences using virtual reality technology or robotics. User-generated images, sexting and 'revenge porn' are new sources of image-based abuse often involving older children. The content of CEM constitutes a crime scene that can help trace offenders and identify victims, but poses challenges for digital forensics. This chapter describes the prevalence and nature of CEM, profiles of offenders and victims, and law enforcement responses. Discussed are definitions of CEM; the relationship between online and offline or contact offending; emerging developments in CEM; the role of transnational policing; and international collaborative and regulatory approaches to suppress CEM.

Keywords: on-line child sex abuse images, child exploitation material, transnational policing, cybercrime

Introduction

The production and distribution of child pornography has a long history, but the advent of the Internet in the 1990s gave new impetus to ‘child pornography’ offenders. The new technology offered unprecedented anonymity, secrecy and efficiency for the widespread sharing and selling of what is more aptly termed Child Exploitation Material (CEM) via networks of those sexually attracted to children. It also provided opportunities for child ‘grooming’ (solicitation and seduction) and the exploitation of vulnerable children. Emerging online criminal networks were trading in CEM (Pierce, 1984; Burgess & Grant, 1988; Flowers 2001; Jenkins, 2001). The Federal Bureau of Investigation’s (FBI) *Operation Innocent Images* launched in 1994 was one of the first to investigate an online CEM group that had shifted its activities to computer bulletin boards and ‘chat rooms’ to share CEM and groom boys. An ‘...alarming new trend: sexual exploitation of children via computers’ was discovered (FBI Archives, n.d.¹). *Terre des Hommes* (2019) citing United Nations (UN) and FBI estimates claims that at any one time 750,000 men worldwide are looking for online sex with children in more than 40,000 public chat rooms.²

The victims of these crimes are children who are subject to sexual exploitation or abuse. The term Child Exploitation Material (CEM) or Child Sexual Abuse Material (CSAM) are preferred to ‘child pornography’ commonly used in the laws of many jurisdictions because it does not convey the gravity of the sexual assault often associated with the production of CEM. For consistency CEM is used throughout this chapter and includes the production, distribution, and possession of CEM; online grooming or active sexual solicitation of children; and sexual exploitation and extortion of children (ECPAT, 2018). This type of offending typically ‘takes place through the Internet or with some connection to the online environment’ (ECPAT Interagency Working Group, 2016, p 34). Facilitated online child sexual assault refers both to the sexual abuse of children that are amplified by information and communication technologies and sexual abuse of children that is committed elsewhere and then repeated by sharing it online through images and videos.

CEM is criminalized across the world; however, law enforcement agencies face substantial challenges in suppressing this crime and prosecuting offenders because of the transnational nature of the offences, and the difficulties in tracing the origin of the images and identifying victims and offenders.

This chapter first discusses the definitions of a ‘child’ and the age of consent. We briefly review what is known about the prevalence of CEM, the characteristics of victims and offenders as well as efforts to suppress the production and distribution of CEM through the

¹ <https://www.fbi.gov/history/famous-cases/operation-innocent-images>

² <https://www.terredeshommes.nl/en/programmes/sweetie-20-stop-webcam-child-sex>

emergence of a growing global web of law enforcement agencies (LEAs), non-government organizations (NGO), industry, academia and international agreements.

Definitions of a child and legal age of consent to sexual activity

Children are vulnerable to CEM because of their lack of cognitive and social development compared to their often-adult offenders. The relationship between the child and offender during sexual abuse is managed and manipulated by the offender(s) using the authority (and physical superiority) they have over the child victim to gratify their sexual (and monetary) needs (WHO, 1999).

The age of a person determines their status as a child or an adult. Generally, those under the age of 18 are defined as children. The 1989 UN Convention on the Rights of the Child (UNCRC) defines a child (Article 1) as a person below the age of 18, unless the laws of a particular country set the legal age for adulthood younger or higher. The Committee on the Rights of the Child, the monitoring body for the Convention, has encouraged States to review the age of majority if it is set below 18 and to increase the level of protection for all children under 18. The 2002 Second Optional Protocol of the UNCRC, specifically, requires states to criminalize the “producing, distributing, disseminating, importing, exporting, offering, selling or possessing” of CEM. Child sexual abuse is not defined by the UNCRC; however, the World Health Organization (WHO) describes child sexual abuse 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. Child sexual abuse is evidenced by this activity between a child and an adult or another child who by age or development is in a relationship of responsibility, trust or power, the activity is intended to gratify or satisfy the need of another person (WHO, 1999, p. 15).

While the age threshold for defining a child is relatively uniform across the world, the legal age of consent to sexual activity varies widely across jurisdictions (from 12 in Angola to 20 years of age in Korea) and may vary within federal systems of government; for example, in Australia, the usual age is 16, but in Tasmania and South Australia, it is set as under 17). Some jurisdictions set a higher age of consent for homosexual relations.

Attitudes to and suppression of sexual activity with children have changed over time and place and this is reflected in shifts in the age of majority and the age of consent (Foucault, 1990; Toulalan, 2014). For example, the United Kingdom (UK) in the *1885 Criminal Law Amendment Act* changed the age of consent from 13 to 16 in response to scandals involving the prostitution of children (Cox, 2017). Over the past century India has changed the age of consent from age 10 to age 12 (in 1892 following the death of an 11-year old bride following rape by her 38-year old husband) then to 16 years (in 1949 driven largely by

concerns about maternal and infant health). Following the widely publicized ‘gang rapes’ of young women in Delhi in December 2012 and Mumbai in August 2013 the Indian Penal Code and related laws were amended to set the age of consent at 18 (Jolly & Kahn, 2016).

A number of African and middle-Eastern countries have no minimum age of consent and ban all sexual relations outside of marriage; consent is tied to marriage and in some cases, children may be married at very young ages. In such jurisdictions and those that define the age of consent for sexual activities at younger ages (e.g., Japan at 13 or the Philippines at 12 years), CEM involving children under 16 but over 12 years of age may be difficult to prosecute, although possession and/or distribution of such images in Australia and many other countries would be unlawful.

Prevalence

Estimating the prevalence of CEM offenders in the population is extremely difficult. Although over ten years old, the US longitudinal National Juvenile Online Victimization study has shed some light on the prevalence of CSA and CEM over time. Fielded in three waves in 2000, 2006 and 2009 (now discontinued), it is based on those arrested for online facilitated sex crimes against children. An increase in arrests (from 2,577 in 2000 to 7,010 in 2006 and 8,144 in 2009) was observed with half of the arrests being for possession of CEM (Walsh, Wolak & Finkelhor, 2012).

A recent review of online child sex offending by NatCen Social Research (2018) observed a large number of images and active websites. For example, Canadian authorities identified over 5 million CEM images over a six-week period. The Australian Centre to Counter Child Exploitation (ACCCE) estimates that over a million CEM websites are currently active and Australian Federal Police (AFP) received over 15, 857 reports in 2018.³ The International Criminal Police Organization (Interpol) Child Sexual Exploitation Image Database (ICSE-DB) network of 53 countries holds over a half a million CEM images, which have helped identify around 11,988 victims and nearly 5, 617 offenders over the eight years to December 2017 (Interpol 2017, p 28). Analysts working for the NGO End Child Prostitution and Trafficking (ECPAT) monitor webpages every five minutes. They reported that every nine minutes a webpage shows an image of child sexual abuse (ECPAT, 2018). The US National Center for Missing and Exploited Children reported the volume of CEM being shared via videos instead of still images has increased tenfold from 312,000 in 2015 to 3.5 million in 2017 (Langston, 2018). The prevalence of CEM in Tor like crypto-markets is unknown.

The UN Special Rapporteur on the sale of children, child prostitution and child pornography estimates that “...the criminal child sexual abuse material-market generates between US\$3 billion and 20 billion annually. Other estimates place the market [for CEM] at US\$250 million per year.” (UNODC 2015, p. 34).

³ See <https://www.accce.gov.au/>

Nature and Severity of CEM Offending

Once seized, CEM is a vital resource for the identification of victims and the prosecution of offenders. Describing and classifying the nature of the CEM is crucial to extract full forensic value from the material stored into various national and international CEM databases. The Interpol Child Abuse Image Database (ICAID), the International Child Sexual Exploitation Database (ICSE-DB), and various national Centers for Missing and Exploited Children (NCMEC) and national databases such as the UK Child Abuse Images Database (CAID) provide CEM libraries essential for tracking images and identifying victims and offenders. In addition, the Internet Watch Foundation (IWF) and International Association of Internet Hotlines (INHOPE - an umbrella organization for national Internet hotlines that report online child sexual abuse and CEM) and other NGOs provide reporting and complaint services for individuals, businesses and others who encounter CEM.

Description of Observed CEM

While it is difficult to assess the scope of the global CEM illicit market, images and other materials monitored and seized by law enforcement and other agencies provide some information on the type of CEM that is produced and circulated. The nature of the images seized has been detailed in a study of 103 online sex offenders arrested by police agencies in Italy, USA, Australia and New Zealand during a joint investigation of the Virtual Global Taskforce For Combating Online Child Sexual Abuse (VGT). Eighty per cent of the children pictured on the seized images were female, but male children appeared on 45% of images. Most of the material included children aged between 2 and 12 years, over half pictured teenagers and just under a quarter, infants younger than 2 years. Perpetrators portrayed on the images were predominantly males aged over 25 years. The ethnicity of both children and perpetrators tended to match the suspects' country of origin, suggesting that the images were produced locally and initially exchanged within the offender's national networks. For 35% of suspects, the most serious images in their possession involved sexual activity between children, and for 47%, sexual assault of children by adults, including penetration and sadistic activities. Fewer than 20% of suspects collected images of children not engaged in sexual activity (Bouhours & Broadhurst, 2011).

The IWF (2017, p. 16) reported that CEM content identified from 2014 to 2017 depicted the most graphic and severe forms of child sexual abuse when younger children were involved. The report noted that since 2014 the percentage of children aged 11 to 15 depicted in child sex abuse imagery had increased from 18 to 43 percent, whilst that of children aged 0 to 10 has decreased from 80 to 55 percent in 2017; girls remain the primary victims. The increase in imagery of 11 to 15-year-olds may be related to the increase in 'self-produced' or user-generated content created using webcams or during live-streaming and subsequently shared widely online.

The same report noted a decrease in the quantity of images showing sexual abuse of children by adults and other children from 43 percent in 2014 to 33 percent in 2017. Images depicting non-penetrative sexual abuse have also shown a decrease since 2014, from 30 to 21 percent. These fluctuations, however, are poor predictors of trends and may reflect countermeasures taken by offenders such as the increased use of encryption and ‘flight’ to crypto-markets rather than a decrease in prevalence.

A recent UK study involving 687 children identified in CEM showed an increase in the number of victims over the 2006-2015 data capture period. Two-thirds of all the images were classified as coercive. Almost two-thirds of the children identified were white females; 44.3% of the images were self-taken and of these most were taken in a coercive relationship (Quayle, Jonsson, Cooper, Traynor, & Svedin 2018, cited in ECPAT 2018, pp. 13). Another study of 3,503 18-year-old Swedish youth indicated that for 6.5% of those who reported sexual abuse, the abuse had been documented in pictures or videos; these children also experienced more severe forms of CSA, such as penetrative sex, recurrent sexual abuse and multiple offenders (Svedin, 2012 cited in ECPAT 2018, pp. 12)

In a dataset of 1,965 cases (from the UK ICSE, NCMEC database of identified children), 61% of cases involved single victims, while images of multiple victims were more likely to involve pubescent children. The majority of cases involved male offenders who were unrelated to the identified child; however, cases with female offenders, younger children or more extreme content were likely to involve family members. In a study of unidentified victims in ICSE database, nearly two-thirds (64.8%) of children were girls, 31.1% were boys and the remaining 4.1% included children of both sexes. Boys were often depicted in content involving more severe abuse. The majority (93.3%) of the children were white. Where age could be determined, the largest group was of pre-pubescent children (56.2%). Across the available databases the proportion of infants abused varied between 6.5-12.4% of all cases (ECPAT, 2018, p. 13).

CEM Severity

A number of CEM classification schemes are in use, but the classification and coding process is fraught by problems of reliability and consistency across classifiers particularly in respect to the age of persons and the degree of indecency (Kloess, Woodhams, Whittle *et al.*, 2019). The most widely used system across the English-speaking world is the COPINE classification and its variants. The COPINE project (Combating Paedophile Information Networks in Europe) was developed in the 1990s for therapeutic and psychological purposes and was used initially to distinguish between child ‘erotica’ (‘artistic’ posing with no sexual activity) and child pornography. It was then adapted to categorize child abuse images in research and legal settings within ten levels of severity (Taylor, Holland & Quayle, 2001).

The (UK) Sentencing Advisory Panel (SAP) then reduced the ten-level COPINE classification to five categories, and provided sentencing guidelines based on these categories – sometimes referred to as the ‘Oliver Scale’.⁴

The Oliver (SAP) Classifications

The five categories of the Oliver scale, as originally devised, are:

1. erotic posing with no sexual activity
2. sexual activity between children, or solo masturbation by a child
3. non-penetrative sexual activity between children and adults
4. penetrative sexual activity between children and adults
5. sadism or bestiality.

The Australian National Victim Image Library (ANVIL) is a reference holding of CEM that has adapted the Oliver (SAP) scale as a means of classifying the severity of CEM and uses a version of Microsoft PhotoDNA to track and identify new CEM. The ANVIL classification system incorporates an additional three categories covering material that is not illegal but is connected to CEM. Category 6 encompasses material featuring any of the activities described by Categories 1 to 5 of the Oliver scale but is not a genuine photograph or does not feature a real child. This includes animé, cartoons and drawings depicting children engaged in sexual poses or activity. Category 7 and 8 cover material directly connected to the exploitation of a child but not illegal in itself and adult pornography. The classification assists Courts to assess an accused’s sexual interest in children.

Victims of CEM: Risk Factors

Research shows that sex, socioeconomic factors and social networking presence impact the risk of victimization; however, poverty is the mediating factor. Generally, victims of CEM are financially poorer than offenders, and often live in disadvantaged locations. The available evidence suggests that numerous cases of child sexual abuse and exploitation occur in developing countries. A typical example is the comparatively wealthier western sex tourist who travels to, says Southeast Asian countries, and engages in child sex offences with local children (Australian Federal Police, 2015). A lack of social security, entrenched inequalities and ineffective child protection practices impact the marginalized populations across the region, where up to one-third of citizens live below the poverty line (United Nations Development Program [UNDP] & ASEAN, 2017). Poor parents perhaps not able to support their family may be driven or enticed into the role of producer of CEM using their own children or paid for access to their children. The sacrifice of a child in return for money may sometimes appear necessary for the survival of the child’s family. Yet, the visibility of child sexual abuse in South-East Asia does not discount its existence amongst other regions (notably West Africa, where the age of consent may be as low as 11 years of age) as well as developed countries.

⁴ From a leading UK case: *R v Oliver, Hartrey and Baldwin* (Times Law Report, 6 December 2002).

Hernandez, Lacsina, Ylade et al. (2018) reviewed English news articles published between 2011-2015 and referring to cybersex cases involving children in the Philippines. They identified 55 articles that reported on cases of live streaming, CEM and ‘sextortion’ involving children from 18 months to 17 years of age. They noted that 72% of victims were female, 24% male and female, and 4% exclusively male. Seven of the cases involved family-run operations, 27 hidden ‘cybersex dens’ mostly in slum areas and eight cases were associated with fake call centers that engaged in online chats or businesses that sold CEM. All the clients were male. One-third of the offenders were foreigners.

Cybersex operations involved uploading sexually explicit images of children, nudity in front of a webcam, and live sexual performances with children or among children. In one operation, snapshots of naked children cost USD50, nudity in front of the webcam cost USD100, and a live sex show among children cost as high as USD500. The children, or parents, got USD10-USD18 per show. Sudden show of increased wealth would arouse suspicion in the community but did not always prompt reporting (Hernandez, et al. 2018, p. 39).

Impact of CEM on victims

Few studies of children who have experienced sexual assault are reported due to ethical concerns. A survey of survivors by the Canadian Centre for Child Protection (2017) found that the online sharing of images and videos of crimes committed against them intensified feelings of shame, humiliation, vulnerability and powerlessness. One survivor explained: ‘The abuse stops and at some point, also the fear of abuse; the fear of the material never ends.’ Another lamented:

The hands-on was horrible. But at the very least it is over and done with. The constant sharing of the abuse will never end; therefore, the reminder of its existence will never end. ... If you ask me, a crime that will never end is worse than one that is over; no matter how much more serious it may appear. That this is something inescapable. That there will never be total absolution” (Canadian Centre for Child Protection, 2017, p. 149).

Survivors of CEM often display behavior consistent with post-traumatic stress disorder (PTSD) (Hannah, Orcutt, Miron & Thompson, 2015). Images can be replicated and shared again. Victims experience anxiety using the Internet because their image may re-appear and they will be traumatized again. This constant re-victimization process and stress impact day-to-day functioning, degrades quality of life, increases potential physiological and mental harm and negatively affects life course (Canadian Centre for Child Protection, 2017). CEM survivors tend to experience high levels of mental illness, heart disease, lower immune system response, behavioral problems, alcohol or drug addiction, and certain cancers and diseases such as liver disease, which often results in shorter average life-span (Gewirtz-Meydan, Walsh, Wolak, & Finkelhor, 2018; Hannah, Orcutt, Miron & Thompson, 2015).

CEM Offenders

Research about online sexual offending is relatively new and has focused on potential links or differences between online and offline child sex offending (e.g. Brown & Bricknell 2018; Henshaw, Ogloff & Clough, 2016; Elliott et al. 2009; Endrass et al., 2009; Webb, Craissati & Keen 2007), sexual addiction (e.g. Henshaw, et al., 2016; Young 2008), childhood sexual abuse experiences and online access to CEM, online grooming behaviors (e.g. Jayawardena & Broadhurst 2007) and studies of victims (e.g. Babchishin, Merdian, Bartels et al., 2018; DeHart, Dywer, Seto, et al., 2016). Samples of offenders are often small and limited to a handful of countries.

Richards (2011, p.1) argued "...perpetrators of sexual crimes against children are not, contrary to widespread opinion, a homogenous group. Rather, there are a number of varied offending profiles that characterize child sex offenders". In part variation occurs because some offenders engage in contact sexual offences including production and/or distribution, while others only view and/or collect CEM (i.e., non-contact child sex offenders). Online only offenders may become child sex contact offenders and exposure to CEM may play a role in shifting their offending. The assumption that CSA offenders are mostly or exclusively paedophile (i.e., sexually aroused only by a child) is not borne out by the variety of sexual predation observed.

The notion of a specific 'type' or 'profile' of online CEM offenders is not supported; however, offenders tend to be white, young, single and unemployed (Babchishin, et al., 2011), although other studies (Brown & Bricknell, 2018) found offenders more likely to be employed. Babchishin et al. (2011) conducted the first review of 27 studies (mostly North American/English language studies released up until 2009) addressing the question of whether online offenders differ from offline offenders. They found that *online* offenders displayed higher sexual deviancy, experienced more psychological barriers to acting on these deviant interests but also exhibited greater victim empathy than contact child sex offenders. Online offenders may be less likely to act on their sexual deviant interests because they wish to avoid the connection or closeness associated with real-life relationships and prefer the emotional distance of images or other material. Noting the novelty of research about online offenders the authors suggest:

One line of inquiry would explore the inhibitors and self-control mechanisms that limit the extent to which online offenders act on their deviant interests. Another line of inquiry would explore the extent to which the emotional distance inherent in pornography use is a core feature of the sexual preference of online offenders (Babchishin, et al., 2011, p.110).

They reiterated the findings about the "...tendency for men to prefer sexual partners of the same race ... a change in the racial distribution of child pornography victims will likely signal an expansion of this deviant market into more racially diverse segments of the male population" (p.110). However, this finding may reflect the limitations of studies largely

restricted to the English language and may also be further obscured by the forensic awareness of online child sex offenders (Bouhours & Broadhurst, 2011; ECPAT, 2018).

Brown and Bricknell (2018) reviewed recent literature about those that view and collect CEM. They identified 49 peer-reviewed studies that provided quantitative data – drawing on official criminal justice data about convicted offenders and online convenience samples. These studies examined demographic (age, ethnicity, marital and parenting status, education and employment) and psychological factors (mental health, cognitive distortions) and offending characteristics (prior offending, and recidivism risk). CEM offenders were predominantly white males, tended to be older than the average offender (i.e. between 35 and 45 years of age) but younger, more often single and better educated than contact sexual offenders. Very few had prior offences for contact sexual offences and generally were less likely to re-offend than contact child sex offenders. The evidence also suggested that CEM offenders “...tend to be less assertive, less dominant and under-socialized” and “...show higher levels of sexual deviancy than contact or mixed sexual offenders and are more likely to fantasize about children”. The study concluded that the ‘profile’ of CEM offenders “...may be different to that of other types of sexual offenders, especially those who commit contact sexual offences against children” (Brown & Bricknell, 2018, p. 9).

Despite inconsistent evidence to support a causal relationship between online and offline sexual abuse of children, various typologies for online and offline sexual offenders have been developed in an attempt to clarify key differences and similarities in their profiles and predicted behaviors. For example, Webster et al. (2012) proposed that some offenders are ‘intimacy-seeking’ and view their communication with children as a consenting relationship compared to ‘hyper-sexualized’ offenders who quickly proceed with sexual communication (see also Armstrong & Mellor, 2013; McGuire & Dowling, 2013). Other typologies focus on the offender’s actions and distinguish between collection, distribution and use of CEM (Corriveau & Greco, 2012; McNally, 2016); or contact versus fantasy driven offenders (Merdian, Moghaddam, Boer, et al. 2016). Although there are several ways of differentiating online offenders, both compared to each other and to offline offenders, a major challenge is determining the difference between offenders who use the Internet as a means of satisfying sexual needs (i.e. offline sexual abuse) and those who use cyberspace to consume and engage in online CEM instead of in real life. Viewing online CEM could provide a ‘safer’ outlet for individuals to fantasize and virtually experience their deviant sexual interests (Corriveau & Greco, 2012). Generally, research highlights the *disinhibiting effects* of the Internet that helps facilitate offending behavior (Merdian, et al. 2016).

Overall research suggests that situational and environmental factors (and the relevance of situational crime prevention strategies) are as important as the probable pathology of offenders for the prevention of CEM online (e.g., Elliot et al., 2009; UNODC 2015; Wortley & Smallbone, 2006).

CEM - Modus Operandi

Victim recruitment

Computer applications (apps) and online games are easily available on a range of devices that younger children (8 to 13 years) use routinely. They include communication apps (e.g. instant messaging services), gaming apps, social media (e.g. Facebook, Instagram) apps or a combination. Most apps have a messaging or chat feature, which provides a way for adults to hide their identity and reach hundreds of children by pretending to be one of their peers (Keating, 2015). Children may be more inclined to share information or content as they feel it cannot be traced back to them through their anonymous account. For example, online gaming platforms *Minecraft*, *League of Legends* and *Fortnite* were used by offenders to communicate directly with children in an attempt to obtain CEM (Boyd, 2018; Cimpanu, 2019; Nurse, 2018).

Games may also be hacked by offenders to allow them to gain access to child players. The 2016 *Pokemon Go* quickly attracted malware that looked like the real game but was in fact used to groom and lure children. *Pokemon Go* used a location function, which was useful for offenders who could arrange to meet their victims in real life (Office of the Children's eSafety Commissioner & ACMA 2016, July 20).

In February 2017, the Canadian Centre for Child Protection issued a warning about the online multi-player gaming site *Roblox* following multiple reports of luring or grooming and sexually explicit chat messages and requests to meet received by younger children younger on the game's chat feature. *Roblox* reviewed the game and added chat-filtering software to find and flag offensive language, used a moderator network to review each image, audio, and video file uploaded to the site, and made sure that the accounts of all users under the age of 13 were defaulted to communicate exclusively with friends (CBC, 2017). Similar warnings about grooming attempts via *Roblox* have been issued in USA, Australia and the UK (International Centre for Missing & Exploited Children, 2017).

While strangers often try to contact children and youth through apps and games, the danger can also come from peers and acquaintances. In 2016, young women and underage girls from at least 70 Australian schools were targeted by users of an online pornography website. While the site was hosted overseas, most of the users were local, some attending the same schools as their victims. Users were largely young men and teenage boys attempting to obtain nude images as well as identifying information of specific 'targets' (name, phone number, school and home address, etc.) to view and share. The Australian Federal Police (AFP) and the Australian Office of the Children's eSafety Commissioner worked together to take down the site, which hosted thousands of images, some falling into the CEM category (Funnell, 2016).

User-generated CEM

User-generated CEM consists of images produced and shared willingly with a few trusted

persons that is then stolen and shared online without the consent of the person who produced the material and sometimes without their knowledge. Many LEAs and INHOPE hotlines now report that the misuse of user-generated images is among the most common complaints handled. The rise of social media is integral to the production and distribution of user-generated CEM material and all content uploaded to networks such as Facebook, Instagram or Snapchat could be considered ‘user-generated.’ Parents may upload ‘innocent’ photos of their children with the intent of showing them only to family and friends; however, these photos and videos can become accessible to others who may be able to subsequently identify young CEM targets (Battersby, 2015). Online predators often collect sensitive information from social network profiles and use it to contact vulnerable children (Maxim et al., 2016).

Sexting and CEM

A key factor for online CEM is the common user-generated act of ‘sexting,’ which involves the sharing of ‘sexually suggestive, nude or nearly nude photo’ (ACMA, 2013, p. 11) of oneself or a girlfriend/boyfriend or another person via a photo app on a smart phone or computer (Keating, 2015). It is not uncommon for older children to engage in this behavior, and 13% of 16 and 17-year-old Australian teenagers reported having engaged in sexting (ACMA, 2013).

Even the consensual sharing of explicit images can constitute an offence and pose legal risks if a child is involved. In many jurisdictions including states of the US and Australia, ‘Romeo and Juliet’ provisions provide a defense to a child sex offence if the participants are teenagers of a similar age in a consensual relationship. Age-difference laws usually specify an age gap (e.g. a two to four-year age gap) but varied greatly as Bieri & Budd (2018) observed in a review of US federal and state laws. However, consensually shared or ‘stolen’ sexualized images distributed via various apps may inadvertently or otherwise enhance and facilitate online CEM (Wolak, Finkelhor, Walsh, & Treitman, et al. 2018). In addition, sexting may lead to ‘sextortion,’ where victims are convinced to provide sexualized user-generated material and, then, under the threat of exposure, compelled to continue providing such images to the offender (Europol, 2013; IOCTA, 2015). Sextortion directly facilitates the production of CEM as it provides offenders with more material and vulnerable targets (UNODC, 2015).

Between October 2013 and April 2016 1,428 reports of sextortion were recorded by the US NCMEC CyberTipline and 78% involved female child victims, 15% involved males with the remaining 7% the gender was unknown (NCMEC, n.d.⁵). In a study of 78 US prosecuted cases all offenders were male, often with prolific repeated offending, while victims were mostly females many child victims were male (Wittes, Poplin, Jurecic, & Spera, 2016). In 2016, a Californian offender, Luis Mijangos, orchestrated many acts of sextortion on

⁵ See <http://www.missingkids.com/theissues/sextortion>

multiple victims. He obtained sexual videos and images from his victims by threatening to expose indecent images or content obtained through deception. He had convinced his victims to download malware that provided him access to their files and assumed control over their device microphones and web cameras thus gaining remote access to their private lives (Wittes et al., 2016).

Finally, hacking and phishing are also an avenue for the production and distribution of online CEM. The hacking of 'big data' sites and websites provide hackers with content such as personal images or online conversations to sell and distribute to others through niche VPNs and other encrypted online platforms. Children are placed at risk if they divulge personal information, private images, or videos through these apps and websites since they lose control of the content once it has been sent or uploaded (Maxim, et al., 2016).

Emerging Technologies

New technologies such as high-speed Internet, file compression, increased CPU speed, live streaming and virtual reality, have improved the quality of CEM and the ease of distributing videos, which have begun to replace photographs. These new technologies make possible the ability to request almost instantaneous, customized material.

Webcamming and Live-streaming

Live streaming of child sexual abuse continues to evolve, and clients are able to order and pay online for criminal services such as customized online child sexual abuse 'on-demand' (IOCTA, 2015; Wolak, 2015). Evidence of the growing monetization of online CEM suggests the emergence of criminal organizations that avoid tools such as web crawlers and hash and URL lists that have traditionally provided ways to identify CEM and to block and or blacklist illegal content from the Internet.

Live streaming offences take place in 'real-time' and do not require the offender to store the material, making it more difficult for law enforcement agencies to acquire digital-evidence (Europol, 2013; 2015; Thorn, 2016). Perpetrators and producers avoid detection by conducting multiple payments of smaller amounts that do not to arouse the suspicion of financial monitoring programs (Europol, 2015). Furthermore, the act of solely 'viewing' streamed material (not storing it) may not always fulfill the legislative requirements of 'possession or production' of CEM material in all jurisdictions (Europol, 2013).

The demand for new 'fresh' material and a customized experience is crucial in understanding the popularity of CEM streaming. Prices of on-demand material (e.g. live streaming or video files) are still significantly higher than dated or generic material but are falling (Europol, 2013; ECPAT, 2017; IWF, 2018). "Live-streamed abuse is not only increasingly common, but also increasingly affordable. Five or six years ago, access to live-streamed abuse cost in the region of \$US50 Today, it is available for \$US15–20. LEAs predict costs will continue to decrease" (WeProtect Global Alliance 2018, p. 12).

Virtual Reality (VR)

The purpose of VR is to live the experience without actually being there and it has the potential to transform the pornographic industry. With the advent of Google Cardboard and Oculus Rift, the VR experience has now become affordable and pornography consumers are among early adopters of this technology (Hussey, 2016; Takahashi, 2016). Rather than the typical voyeuristic, third person standpoint in traditional pornography, VR pornography is a first-person point-of-view system that delivers an intimate viewing experience for users (Takahashi, 2016). Additional sexual peripherals (i.e., sex toys that recreate the sense of touch) increase the sense of intimacy and realism and can be programmed to respond to an individual's movements or the feedback from a video or livestream (Cooper, 2015).

Research into the viewing of CEM by non-contact pedophiles has suggested that they are less likely to offend in the real world because of moral, personal and legal constraints (Brown & Bicknell, 2018). The VR CEM enhanced experience of intimacy and realism may break down these barriers and entice an online offender to become a child sex contact offender (Rutkin, 2016; Maras & Shapiro, 2017). Although VR or child sex dolls could be useful as a treatment for pedophilia, it may also encourage some offenders to enhance their experience by incorporating live streaming of actual child abuse with the tactile experience promised by such technologies. Brown & Shelling (2019) in a review of the limited literature on the therapeutic benefit of child sex dolls including robotic versions note there is '...no empirical evidence to support the assertion that sex dolls (whether adult or child) reduce the likelihood of sexual violence'.

Distribution of CEM

Little is known about CEM networks and their relationships with other criminal enterprises or how trust is acquired and maintained in the virtual world. Illicit markets, such as that for CEM, require consumers to trade tools or illicit images before accessing the network.

The IWF remarked, "...criminals are increasingly using masking techniques to hide child sexual abuse images and videos on the internet" (IWF, 2016, p. 19) and:

"...online-facilitated CSA are increasingly disguising digital pathways leading to indecent and illegal content online through legitimate and legal Internet sites. ... This reflects a trend for illegal content being hidden more professionally, shifting away from peer-to-peer networks into deeper parts of cyberspace, with a higher volume of CSA material being shared and published in forums on the darknet" (NatCen Social Research, 2018: 15).

The 'Darknet' or Tor based crypto-markets are now among the major platforms used by online offenders due to the enhanced anonymity provided for creating and distributing online CEM. Many large crypto-markets such as *Dream Market* prohibit the posting or sale of CEM on their sites and peer-to-peer VPNs and niche Tor like markets will continue to be

preferred methods to communicate and distribute CEM despite LEA efforts to de-anonymize these illicit networks and identify offenders. Crypto-currency block-chain ledgers have been recently identified as a means of storing and concealing CEM (Sward et al., 2018; Matzutt, Hiller, Henze, et al., 2018).

Responses to CEM

International law enforcement co-operation

Differences in legal definitions of offence and in the age of consent confound cross-national and international efforts to suppress CEM because many states require legal equivalence before providing mutual legal assistance (MLA). The quickening of MLA and the creation of common legal definitions of CEM are essential to respond to the cross-national nature of many CEM offences as is typical of cybercrime offences in general. This is because the offender, victim and CEM may be located in different jurisdiction.

The first international treaty seeking to harmonize national laws and increase cooperation to address cybercrime was signed in 2001 and came into force in 2004. The Council of Europe (CoE) *Convention on Cybercrime (Budapest Convention)* outlawed ‘child pornography’ (Article 9) by requiring member states to make it illegal to produce, distribute, offer, procure, or possess child pornography via computer or media storage device. The *Budapest Convention* is a key instrument for international law enforcement cooperation, and provides for the extradition of suspects, the disclosure and preservation of computer and traffic data, real time traffic data collection, trans-border access to stored computer data and the interception of CEM.

The *Budapest Convention* has been adopted by 67 states around the world including all 47 states in Europe. However, China, Brazil, the Russian Federation and India among others have not signed the Convention limiting its scope in assisting with CEM offences that may involve offenders and victims from these jurisdictions.

Since the *Budapest Convention*, concerns about the increasing availability of child pornography and other serious forms of sexual abuse and sexual exploitation of children through the use of new technologies and the Internet have intensified. To keep pace with new technologies the CoE in 2007 strengthened laws aimed at suppressing all forms of CEM enacting the *Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse* or the *Lanzarote Convention*. The *Lanzarote Convention* focuses on ensuring the protection of children through the prevention of abuse and exploitation, assistance for victims, punishment of perpetrators, and promotion of national and international law enforcement cooperation. Crucially the *Convention* stressed the increased use and inherent danger of information technologies in the exploitation of children. The *Lanzarote Convention* for the first time in an international treaty established the offence of solicitation or grooming of children for sexual purposes as a standalone offense considering

the Internet and mobile phones among the most dangerous methods of grooming children (International Centre for Missing & Exploited Children, 2017).

Following the initiative of the *Lanzarote Convention*, the European Parliament and the Council of the European Union passed in 2011 a European Union (EU) Directive on combating the sexual abuse and sexual exploitation of children and child pornography (2011/92/EU) to strengthen efforts to suppress child sex abuse and CEM. The EU's Directive on CEM and child sex abuse provides a comprehensive description of the proscribed behaviors or offences and seeks to improve protection based on a greater understanding of the risks of CEM facilitated by the Internet.

The USA, UK, Australia, Canada, New Zealand (NZ) and many other states have long-established laws aimed at suppressing child sex abuse and CEM and regularly update laws to keep pace with changes in information communication technology (ICT), in particular responding to the increasing presence of encryption in messaging, social media and Voice over Internet Protocol (VoIP) services. The AFP report that 90% of telecommunications information now intercepted by them uses some form of encryption (Australia, Minister for Home Affairs, 2018). In response to the rapid uptake of encrypted ICT by terrorists and other serious offenders such as producers of CEM a controversial new Australian law, *The Telecommunications and Other Legislation Amendment (Assistance and Access) Act*, was passed in 2018 to provide law enforcement with additional powers to decrypt communications between high-risk offenders via computer access and search warrants. The *Assistance and Access Act* increased penalties for suspects who decline to provide passwords or de-encryption keys and requires assistance from telecommunication companies in Australia and abroad. Enhanced computer access powers will enable Australian LEAs to assist overseas partners connected through Australia's mutual legal assistance framework because '...computers, communications and encryption are now global and perpetrators of crimes and terrorist acts have a global reach through these mediums' (Australia, Minister for Home Affairs, 2018). There were, however, widespread objections from the cybersecurity and ICT industry that claimed that the risks inherent in 'backdoor' de-encryption access could also assist criminals and drive offenders to non-commercial encryption methods (Hayman, 2018).

The absence of a universal treaty on CEM is a significant barrier but is partially addressed by the UN *Transnational Organized Crime Convention* (UNTOCC) or the *Palermo Convention* that came into effect in 2003 and was signed by 147 states including China, Russia, India and Brazil who, as noted, are not signatories to the *Budapest Convention* on Cybercrime. The UNTOCC is the key multi-lateral treaty addressing organized crime, and can be invoked in cases where an organized crime group uses CEM. However, the offences to which it applies must attract a penalty of four years or more prison in the countries affected. This threshold limits obligatory cooperation to only the most serious CEM production offences, although police-to-police co-operation in less serious matters often

occurs informally. Three additional protocols extend the remit of the UNTOCC. These address trafficking in firearms, people smuggling and trafficking in persons. The *Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children* signed by 117 countries including China, Russia, India and Brazil focuses on the exploitation of trafficked persons and includes "...the exploitation of the prostitution of others or other forms of sexual exploitation, forced labour or services, slavery or practices similar to slavery, servitude or the removal of organs" (UNTOCC, Article 3). The UNTOCC combined with the efforts of Interpol and regional LEAs suggest that a seamless web of law enforcement cooperation to suppress CEM is possible.

The apprehension of offenders and suppression of CEM

Law enforcement officials attribute CEM offences to specific individuals by connecting the offence to a particular digital device and the user of the device, and then tracing illicit acts back to the source such as an IP address and a person. However, anonymity and encryption make the identification of the devices and/or persons responsible for the cybercrime difficult (Lin, 2016).

CEM offences do not usually involve computer trespass but rather the presence of illegal content. Consequently, covert strategies are useful to identify and disrupt the criminal conspiracies and enterprises that drive CEM online networks. Proactive policing such as police posing as CEM offenders to gain access to distribution and collector sites or posing as vulnerable children have been fruitful (Jayawardene & Broadhurst 2007) but have become less effective over time. More recent network investigation techniques and undercover investigations have become the norm (Walsh, Wolak & Finkelhor, 2012). These new methods play an increasingly important role in the suppression of CEM as cases such as *Playpen*, *Sweetie* and *Child's Play* illustrate.

Sweetie

The Dutch children's rights organization Terre des Hommes sought to address the growing problem of webcam sex tourism through the *Sweetie* operation in 2013. Terre des Hommes created a ten-year old Filipino girl *Sweetie* as a fictional online vulnerable child whose role was to collect data (e.g. detect IP addresses) from individuals who contacted *Sweetie* to solicit webcam sex. She engaged in discussion with potential child sex predators but was not programmed to undress, perform sexual acts or show sexual organs and thus did not meet the legal elements of a child sex offence in most jurisdictions (Schermer, Georgieva, Hof & Koops, 2016, p 83). The *Sweetie* 'sting' operation ran for three months and led to the investigation of around 1,000 potential offenders from 71 countries (Açar 2017; Schermer, et al., 2016). Following amendments to the Netherlands Criminal Procedure Law in 2016, Dutch police were able to use a 'virtual child' in CEM investigation and adapted methods that avoid legal challenges associated with entrapment. The legality of lures is less crucial in common law jurisdictions (Australia, USA, Canada, New Zealand [NZ] and the UK) because matters of subjective intent (i.e. *mens rea*) are given more weight and interaction

with an avatar or similar may result in offences of attempted child sex offending.

Taskforce Argos and Child's Play

Queensland Police specialist child protection unit *Taskforce Argos* was established in 1997 and conducted successful operations against child pornography because of its extensive legal powers. Similar to a 'controlled operation' commonly used to suppress illicit drug importation and distribution, these powers allow investigators' to undertake undercover operations that involve 'controlled' criminality. This enabled *Taskforce Argos* to undertake operations against CEM networks by joining and engaging with the criminal conspiracies engaged in the production and distribution of CEM. *Argos* was able to use a uniquely powerful investigative strategy not available in other jurisdictions (Bleakley, 2018; Høydal, Stangvik & Hansen 2017).

A common investigative method was to impersonate persons less than 18 years on online chat sites that allow users to 'randomly' chat or socialize with strangers without the need to register such as *Omegle* or *Chatroulette*. If their conversational partner attempted to groom or coerce the investigators' child persona and arranged to meet with the *Argos* agents' child persona, the agents contacted the local authorities and the predator was apprehended by police assigned to observe the meeting (Bleakley, 2018). However, *Argos* also employed a more controversial investigative techniques such as the brief but potent covert takeover of a CEM website.

In 2017, *Taskforce Argos* conducted a covert operation that removed *Child's Play* and *Giftbox*, two large CEM distribution websites operating in Tor crypto-markets. *Child's Play* had been operational in 2016-17 and at its peak had over one million registered users sharing and viewing content (Høydal, Stangvik & Hansen, 2017). *Argos* agents were able to identify and quietly arrest the leaders of both websites, Benjamin 'WarHead' Faulkner and Patrick 'CrazyMonk' Falte, and obtain their administrative passwords. *Argos* officers assumed the identity of Faulkner and actively published CEM to the website to allay any suspicion. During active posting as CEM distributors, *Argos* investigators were able to participate in and view private conversations between users to build a profile of individual members and the likely locations. After several months, *Argos* removed the website and the information obtained in the clandestine operation led to the arrest of many more people than would otherwise have been possible. *Child's Play* had 3-4000 active users and over 100 producers of CEM and led to the rescue or identification of over 100 children (Knaus, 2017). However, controversy remains because *Argos*, for a short time, operated a CEM market and potentially re-victimized the children involved. This was also the case of the earlier FBI takedown of *Playpen* an operation that also raised questions about the methods used by law enforcement in searches of hidden encrypted websites.

Playpen and Network Investigative Techniques

Operation Pacifier, an FBI investigation applying similar methods used by *Taskforce Argos*, led to the shutdown of a notorious Tor based CEM website, *Playpen*, that operated between August 2014 and February 2015. *Playpen* hosted over 20,000 sexual images or videos of children from a server in Virginia, and featured on its home page "...two images depicting partially clothed prepubescent females with their legs spread apart" (U.S. v. Kim, p 4; note 15⁶). The FBI operated the site for two weeks after identifying the site owners' IP address. Malware enabled 'Network Investigation Techniques' (NIT) were used to hack the computers of visitors accessing the CEM via Tor leading to 900 arrests and the conviction with lengthy sentences of three of the principle operators, including the website creator Steven Chase.

Apart from criticism that the FBI operation required the continued distribution of child pornography, the nature of the NIT warrant has been challenged by a number of alleged *Playpen* users (some 60 cases in all with only a few successful in excluding evidence). Justice PK Chen in November 2017 further addressed the validity of the NIT warrant in *US v Kim* in the New York District Court. The defendant, Yang Kim, sought to suppress the evidence obtained using these NITs for his indictment for the possession of child pornography from *Playpen* claiming they constituted a breach of his 4th Amendment constitutional right to not be subject to unreasonable search and seizures. It was further argued by the defendant that the warrants obtained by the FBI misrepresented the grounds for probable cause. Although the defendant's suppression motion was denied, the FBI declined to reveal the full details of the techniques used to search and transmit information to the FBI server from computers logged into the *Playpen* website. The methods enabled the identification of the computer's actual IP address, host name, time stamp and media access control (MAC) address as well as the type of operating system and username on the computer.

Other methods of identifying CEM offenders through malware such as Torsploit that identify a user's real IP address and forward to a FBI server with a timestamp can also be used with NIT to assist in the tracing of CEM on-line users (Cimpanu, 2016). These methods force CEM distributors to become more cautious and invest in methods to identify LEA malware on the darknet. The combination of honeypot, technical 'hacks', anticipation of displacement or migration of users and vendors to new darknet markets combined with attempts to disrupt and undermine trust in these markets illustrate the complexity of the measures needed to suppress such resilient darknets (Afilipoaie & Shortis, 2018).

In 2017 *Operation Bayonet*, a joint FBI, Dutch National High Tech Crime Unit and Europol taskforce used similar infiltration methods to takeover the then largest darknet market *AlphaBay* and briefly operate *Hansa* a smaller related market. As these markets focused on illicit drugs, malware, stolen credentials and other contraband rather than CEM these methods did not attract the level of controversy associated with *Playpen* or *Child's Play*.

⁶ U.S. v. KIM, No. 16-CR-191 (PKC) available from <https://www.leagle.com/decision/infcdco20171113f28>

A Global Regulatory Challenge

The suppression of internet-driven CEM is a major challenge for law enforcement agencies across the globe and a leading example of the response to the transnational nature of cybercrime. Effective alliances have been formed across nations to share intelligence and prosecute the most serious CEM offences. NGOs such as INHOPE and ECPAT along with increasing engagement from industry have begun to increase the risks of detection for CEM offenders. In 2015, INHOPE launched ICCAM (I-''See''(c)-Child-Abuse-Material) that allow the hotlines network to process complaints from the public about illegal CEM. Complaints that identify a suspicious URL are entered into ICCAM system, which then crawls the URL, captures CEM images and passes to a centralized database provided by INTERPOL's Child Sexual Exploitation Image database (ICSE-DB). Cases are then investigated and evidence identified through image analysis, specialist and routine policing (McKay, Swaminathan, Guo & Wu, 2008; Danis, Tyshetskiy, & Wilson, et al., 2018).

The Virtual Global Taskforce (VGT) is another example of a global response to CEM. Established in 2003 to help respond to and investigate serious CEM cross-border cases, VGT coordinates investigative responses to multinational child exploitation material cases and uses information provided by INHOPE, ECPAT and other civil society groups as well as Interpol's ICSE-DB. Over 1,000 investigations have been completed to date. Fourteen agencies including INTERPOL and Europol are actively engaged, often in collaboration with the FBI's Violent Crimes Against Children (VCAC) unit as well as LEAs in Australia, NZ, Italy, UK, Switzerland, Canada, Republic of Korea, Netherlands, Colombia, Philippines and the United Arab Emirates. Promising new image recognition technology, network investigation techniques and web monitoring tools could further strengthen the capacity of LEAs and NGOs to suppress CEM.

Enhancing Forensic Data Capture of CEM

The ICSE-DB now in its fourth iteration has been enhanced to improve connectivity across national CEM databases. The ICSE-DB allows LEAs, especially child protection specialists, to use image comparison software to identify victims, offenders and likely places through the forensic analysis of images and hashes. The expansion of the ICSE-DB to more countries is needed especially in the developing world; however, many jurisdictions also need to reform the law in relation to child sexual abuse and CEM. Many poorer nations require technical assistance to create the computer infrastructure, connectivity and expertise needed to operate a national CEM database. As more jurisdictions become capable of identifying victims and offenders, it is likely that offenders will shift their operations to the most vulnerable jurisdictions and populations.

While CEM perpetrators embrace new technologies that allow them to escape detection, law enforcement has also benefited from recent development in image recognition. Microsoft's PhotoDNA is designed to recognize similar images and has been widely used by police agencies across the world to identify victims found in CEM since 2009. PhotoDNA and a

recent enhancement PhotoDNA Video have become widely used by online services, media providers and law enforcement who apply the tool to seized CEM stored in databases to help identify and trace offenders and victims of child sexual assault. The method developed by the Dartmouth College vision laboratory computes a specific hash value (similar to a fingerprint) for images, video and audio files allowing CEM images to be uniquely identified. The PhotoDNA hash allows law enforcement to match the hash value with images held in CEM databases across the world and to prioritize cases those are new and/or involve ongoing abuse (Farid, 2016).

The application of deep machine learning to CEM image recognition and classification enables researchers using a variety of approaches, notably Convolutional Neural Network best suited to analyze visual images, to manage the increasing scale of CEM available on line (Danis, Tyshetskiy, & Wilson, et al., 2018). The application of Artificial Intelligence (AI) to enhance data capture from child sex abuse images could enable LEAs to improve the availability of forensic intelligence and evidence for the first time on a sufficient scale to impact on CEM distribution networks. These novel approaches have the advantage to reduce human exposure to risks of tertiary victimization through the need for INHOPE, Interpol and local LEA's to repeatedly view and classify CEM.

Conclusion

A daunting challenge for LEAs, educational institutions, communities and parents is how the overlap between licit 'adult' pornography and the child sex abuse (and child 'erotica' [sic]) business can blur boundaries and normalize some forms of CEM. Implicit in responding to the risk of CEM is the need for the education of parents, children and the community. The work of NGOs such as INHOPE, ECPAT and others is crucial in the education process and can be amplified through new institutional responses, such as Australia's E-Safety Commission and UNODC's initiatives such as the E4J (Education for Justice initiative) project that promotes the training of cybercrime investigators and the production of child friendly e-safety materials.

In a recent review of law enforcement efforts to suppress CEM, ECPAT recommended more investment in the development and maintenance of a national database of CEM in each country and the routine analysis of national and trans-national trends in CEM. A critical step in improving the monitoring of CEM is the need to standardize the variables that are collected, stored and analyzed, and to create uniform metrics that effectively measure change in the prevalence, frequency, nature and risk of CEM, especially in highly vulnerable countries increasingly becoming the target for CEM criminal enterprises. This requires constant dialogue across communities about what constitute key metrics on CEM (ECPAT, 2018). A positive step would be to continue to promote participation in research by LEAs and to invest in novel uses of new technologies that can help address the rapid scaling up of CEM now encountered. These include methods to help de-anonymize CEM crypto-markets and the crypto-currencies used to purchase CEM, computer vision and

image recognition techniques that enable rapid forensic extraction of evidentiary material, and research that explores the countermeasures or ‘forensic awareness’ of the producers and distributors of CEM.

The scale and depravity of on-line child sexual exploitation images may be at its zenith but the risks of detection of the criminals have increased. However, the source of these images, crimes of domination remain entrenched and continue to offer opportunities for abuse and profit. A broad approach linking government, NGO’s, industry, LEAs and academia with community engagement in child safety has emerged. Albeit imperfectly the comity realized by these cooperative endeavours at the international and local level have improved awareness and helped disrupt the activities of CEM producers and distributors. As with other crimes, displacement to more vulnerable jurisdictions are likely as criminal enterprises seek out ‘fresh’ CEM and new Internet safe havens.

REFERENCES

- Açar, K. V. (2017). Webcam child prostitution: An exploration of current and futuristic methods of detection. *International Journal of Cyber Criminology*, 11(1), pp. 98-109.
- Afilipoaie, A., & Shortis, P. (2018). Crypto-Market Enforcement-New Strategy and Tactics. *Policy*, 54, 87-98.
- Armstrong, J. & Mellor, D. (2013). Internet child pornography offenders: An examination of attachment and intimacy deficits. *Legal and Criminological Psychology*, 21(1), pp.41-55.
- Australian Federal Police (AFP) (2015). Annual Report 2014-15, Commonwealth of Australia, Canberra. Retrieved from: <http://www.afp.gov.au/~media/afp/pdf/a/afp-annual-report-2014-2015.pdf>
- Australia (Minister for Home Affairs), (2018). Explanatory Memorandum - Telecommunications and other legislation amendment (Assistance and Access) Bill 2018. Commonwealth of Australia. Retrieved from: <https://www.legislation.gov.au/Details/C2018A00148>
- Australian Communications and Media Authority, (2013). Like, Post, Share: Young Australians' Experience of Social Media. Retrieved from <https://www.acma.gov.au/~media/mediacomms/Report/pdf/Like-post-share-Young-Australians-experience-of-social-media-Quantitative-research-report.pdf?la=en>
- Babchishin, K. M., Hanson, K. R., & Hermann, C. A. (2011). The characteristics of online sex offenders: A meta-analysis. *Sexual Abuse: A Journal of Research and Treatment*, 23, pp. 92-123.
- Babchishin, K., Merdian, H., Bartels, R. & Perkins, D. (2018). Child Sexual Exploitation Materials Offenders. *European Psychologist*, 23(2), pp.130-143.
- Battersby, L. (2015, September 30). Millions of social media photos found on child exploitation sharing sites. *The Sydney Morning Herald*. Retrieved from: <http://www.smh.com.au/national/millions-of-social-media-photos-found-on-child-exploitation-sharing-sites-20150929-gjxe55.html>
- Bierie, David & Budd, Kristen. (2018). Romeo, Juliet, and Statutory Rape. *Sexual Abuse: A Journal of Research and Treatment*. 30 (3), 296-321.

Bleakley, P. (2018). Watching the watchers: Taskforce Argos and the evidentiary issues involved with infiltrating Dark Web child exploitation networks", *The Police Journal: Theory, Practice and Principles*. Retrieved from: <https://journals.sagepub.com/doi/full/10.1177/0032258X18801409>

Bouhours, B. & R. Broadhurst (2011). On-line Child Sex Offenders: Report on a Sample of Peer to Peer Offenders Arrested between July 2010-June 2011 (December 15, 2011). Retrieved from SSRN: <http://dx.doi.org/10.2139/ssrn.2174815>

Boyd, C. (Oct 2, 2018). Fortnite gamers targeted by data theft malware. Malwarebytes LABS, Retrieved from: <https://blog.malwarebytes.com/cybercrime/2018/10/fortnite-gamers-targeted-by-data-theft-malware/>

Brown, R. & S. Bricknell (2018). What is the profile of child exploitation material offenders? *Trends & Issues in crime and criminal justice*, No. 564. Canberra: Australian Institute of Criminology.

Brown R. & Shelling J. (2019). *Exploring the implications of child sex dolls*. Trends & issues in crime and criminal justice No. 570. Canberra: Australian Institute of Criminology. Retrieved from <https://aic.gov.au/publications/tandi/tandi570>

Burgess, A. W. & C. A. Grant (1988). *Children Traumatized in Sex Rings*. Arlington, VA: National Center for Missing & Exploited Children.

Canadian Centre for Child Protection (2017). *Survivors Survey - Full Report 2017*. Retrieved from: https://www.protectchildren.ca/pdfs/C3P_SurvivorsSurveyFullReport2017.pdf

CBC News (2017). Child protection group warns parents about luring, explicit chat on game site Roblox. *CBC News*. Retrieved from: <https://www.cbc.ca/news/canada/manitoba/winnipeg-roblox-luring-warning-1.3997258>.

Cimpanu, C. (Jan 16, 2019). Fortnite security issue would have granted hackers access to accounts, *Zednet*. Retrieved from <https://www.zdnet.com/article/fortnite-security-issue-would-have-granted-hackers-access-to-accounts>

Cooper, D. (2015). Adult Themes: The rise and fall of America's first digital brothel. *Engadget*. Retrieved from: <https://www.engadget.com/2015/02/26/adult-themes-digital-brothel/> [Accessed 1 Feb. 2019].

Cox, P. (2017). Blamed for being abused: an uncomfortable history of child sexual exploitation, *The Conversation*, August 17, 2017. Retrieved from:

<http://theconversation.com/blamed-for-being-abused-an-uncomfortable-history-of-child-sexual-exploitation-82410>

Corriveau, P., & Greco, C. (2012). Online Predators and Cyberspace. *Media Kit on Sexual Assault*. Retrieved from: <https://www.inspq.qc.ca/en/sexual-assault/fact-sheets/online-pedophilia-and-cyberspace>

Dalins, J. Tyshetskiy, Y. C. Wilson, M. J. Carman & D. Boudry, (2018) 'Laying foundations for effective machine learning in law enforcement. Majura - A labelling schema for child exploitation materials', *Digital Investigation*, 26, pp. 40-54

DeHart, D., Dwyer, G., Seto, M., Moran, R., Letourneau, E. & D. Schwarz-Watts. (2016). Internet sexual solicitation of children: a proposed typology of offenders based on their chats, e-mails, and social network posts. *Journal of Sexual Aggression*, 23(1), pp.77-89.

ECPAT Interagency Working Group, (2016). 'Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse: Adopted by the Interagency Working Group Sexual Exploitation in Luxembourg', 28 January 2016, Retrieved from: <http://luxembourgguidelines.org/english-version/> .

ECPAT International (2017). *SECO Manifestations - Live streaming of child sexual abuse in real-time*. Bangkok. Retrieved from: https://www.ecpat.org/wp-content/uploads/legacy/SECO%20Manifestations_Live%20streaming%20of%20child%20sexual%20abuse%20in%20real-time_0.pdf

ECPAT International (2018). Trends in online child sexual abuse material, April 2018, Bangkok: ECPAT International, Bangkok. Retrieved from: <https://www.ecpat.org/wp-content/uploads/2018/07/ECPAT-International-Report-Trends-in-Online-Child-Sexual-Abuse-Material-2018.pdf>

Endrass, J., F. Urbaniok, L.C. Hammermeister, C. Benz, T. Elbert, A. Laubacher, & A. Rossegger (2009). The consumption of Internet child pornography and violent and sex offending, *BMC Psychiatry*, Vol 9, pp. 43-49.

Elliot, A., A.R. Beech, R. Mandeville-Norden, & E. Hayes (2009). 'Psychological profiles of Internet sexual offenders: Comparisons with contact sexual offenders', *Sex Abuse: A Journal of Research and Treatment*, Vol 21 (1), pp. 76-92.

Europol (2013). Threat Assessment of Child Sexual Exploitation and Abuse, *Child Exploitation and Online Protection Centre [CEOP]*, United Kingdom. Retrieved from: https://www.norfolkscb.org/wp-content/uploads/2015/03/CEOP_Threat-Assessment_CSE_JUN2013.pdf

Europol (2015). *Copyright European Financial Coalition against Commercial Sexual Exploitation of Children Online*. EUROPOL. Retrieved from: <https://www.europol.europa.eu/publications-documents/commercial-sexual-exploitation-of-children-online>

Farid, H. (2016). *Digital Forensics*, MIT Press, Cambridge Massachusetts

Flowers, R. B. (2001). The sex trade industry's worldwide exploitation of children. *The Annals of the American Academy of Political and Social Science*, 575(1), pp. 147-157.

Foucault, M. (1990). *The history of sexuality: An introduction*, volume I. [Trans. Robert Hurley]. New York: Vintage.

Funnell, N. (2016, August 17). Exclusive: Students from 71 Australian schools targeted by sick pornography ring. *News.com.au*. Retrieved from: <https://www.news.com.au/lifestyle/real-life/news-life/students-from-70-australian-schools-targeted-by-sick-pornography-ring/news-story/53288536e0ce3bba7955e92c7f7fa8da>

Gewirtz-Meydan, A., Walsh, W., Wolak, J., & Finkelhor, D. (2018). The complex experience of child pornography survivors. *Child abuse & neglect*, 80, pp. 238-248.

Hannan, S., Orcutt, H., Miron, L. & Thompson, K. (2015). Childhood Sexual Abuse and Later Alcohol-Related Problems: Investigating the Roles of Revictimization, PTSD, and Drinking Motivations Among College Women. *Journal of Interpersonal Violence*, 32(14), pp. 2118-2138.

Hayman, Lily Hay, (2018). Australia's Encryption-Busting Law Could Impact Global Privacy, *Wired*, Retrieved from: https://www.wired.com/story/australia-encryption-law-global-impact/?mbid=email_onsiteshare

Henshaw, M., Ogloff, J. & J. Clough (2015). Looking Beyond the Screen: A Critical Review of the Literature on the Online Child Pornography Offender. *Sexual Abuse: A Journal of Research and Treatment*, 29(5), pp. 416-445.

Hernandez, Sandra C. L., S., A. C. Lacsin, M. C. Ylade, J. Aldaba, H. Y. Lam, R. Estacio, Jr. & A. L. Lopez (2018). Children Online in the Philippines: A Review of Online News and Articles, *Acta Medica Philippina*, 52 (4), pp. 305-311.

Høydal, H. F., E. O. Stangvik & N. R. Hansen (2017). Breaking the Dark Net: Why The Police Share Abuse Pics to Save Children, *Verdens Gang* p, 1-28. Retrieved from:

<http://nodabase.net/cases/breaking-the-darknet-why-the-police-share-abuse-pics-to-save-children/>

Hussey M. (2016, February). A deep dive into the business of virtual reality porn. *The Next Web*. Retrieved from <https://thenextweb.com/evergreen/2017/09/05/a-deep-dive-into-the-business-of-virtual-reality-porn/>

Interpol, (2017). *Interpol Annual Report 2017*. Retrieved from: <https://www.interpol.int/News-and-media/Publications2/Annual-reports2>

International Centre for Missing & Exploited Children (2017). *Online Grooming of Children for Sexual Purposes: Model Legislation & Global Review*. 1st ed. [ebook] The Koons Family Institute on International Law & Policy. Retrieved from: https://www.icmec.org/wp-content/uploads/2017/09/Online-Grooming-of-Children_FINAL_9-18-17.pdf

Internet Watch Foundation (2017). *Trends in Online Child Sexual Exploitation: Examining the Distribution of Captures of Live-streamed Child Sexual Abuse*. Retrieved from: <https://www.iwf.org.uk/sites/default/files/inlinefiles/Distribution%20of%20Captures%20of%20Live-streamed%20Child%20Sexual%20Abuse%20FINAL.pdf>

Internet Organised Crime Threat Assessment, Europol (2015). *Online Child Sexual Exploitation*. Retrieved from <https://www.europol.europa.eu/iocta/2015/online-child-exploit.html>

Jayawardena, K. & R. Broadhurst, (2007). Online Child Sex Solicitation: Exploring the feasibility of a research 'sting', *International Journal of Cyber Criminology*, 1(2): pp. 228-248.

Jolly, J. & U. Khan (2016). *Rape Culture in India: The Role of the English-Language Press*, Shorenstein Center on Media, Politics and Public Policy, Harvard Kennedy School Discussion Paper Series #D-102. Retrieved from: <https://shorensteincenter.org/rape-culture-india-english-language-press/>

Keating, F. (2015, October 29). Online grooming: New trends in online sexual abuse. *International Business Times*. Retrieved from <http://www.ibtimes.co.uk/online-grooming-new-trends-online-sexual-abuse-1526146>

Knaus, C. (October 7, 2017). Australian police sting brings down paedophile forum on dark web, Retrieved from <https://www.theguardian.com/society/2017/oct/07/australian-police-sting-brings-down-paedophile-forum-on-dark-web>

Richards K. (2011). Misperceptions about child sex offenders. *Trends & issues in crime and criminal justice*, No. 429. Canberra: Australian Institute of Criminology. Retrieved from <https://aic.gov.au/publications/tandi/tandi429>

Kloess, J. A. Woodhams, J., Whittle, H., Grant, T., & Hamilton-Giachritsis, C. E. (2019). The Challenges of Identifying and Classifying Child Sexual Abuse Material', *Sexual Abuse*, 31(2), pp. 173–196.

Langston, J. (2018). How PhotoDNA for Video is being used to fight online child exploitation. *Microsoft on the Issues*. Retrieved from: <https://news.microsoft.com/on-the-issues/2018/09/12/how-photodna-for-video-is-being-used-to-fight-online-child-exploitation/> [Accessed 31 Jan. 2019].

Lin, P. (2016). Is it wrong for victims of cyber-crime to hack back? *World Economic Forum*. Retrieved from: <https://www.weforum.org/agenda/2016/09/is-it-wrong-for-victims-of-cyber-crime-to-hack-back/>.

Maras M.H. & Shapiro L.R, (2017). Child sex dolls and robots: More than just an uncanny valley. *Journal of Internet Law* 21(5): 3–21.

Matzutt, R., Hiller, J., Henze, M., Ziegeldorf, J. H., Müllmann, D., Hohlfeld, O., & Wehrle, K. (2018, February). A quantitative analysis of the impact of arbitrary blockchain content on bitcoin. In *Proceedings of the 22nd International Conference on Financial Cryptography and Data Security (FC)*. Springer.

Maxim, D. Skinner, K., Orlando, S. & R. Broadhurst (2016). *Online Child Exploitation Material – Trends and Emerging Issues*, Research Report of the Australian National University Cybercrime Observatory and Office of the Children's eSafety Commissioner (November 4, 2016). Canberra. Retrieved from: SSRN: <https://ssrn.com/abstract=2861644> or <http://dx.doi.org/10.2139/ssrn.2861644>

McKay, C., Swaminathan, A., Gou, H., & M. Wu (2008, March). Image acquisition forensics: Forensic analysis to identify imaging source. In *2008 IEEE International Conference on Acoustics, Speech and Signal Processing*, pp. 1657-1660.

Merdian, H., Moghaddam, N., Boer, D., Wilson, N., Thakker, J., Curtis, C. & Dawson, D. (2016). Fantasy-Driven Versus Contact-Driven Users of Child Sexual Exploitation Material: Offender Classification and Implications for Their Risk Assessment. *Sexual Abuse: A Journal of Research and Treatment*, 30(3), pp. 230-253.

McGuire, M., & Dowling, S. (2013). Cyber-enabled crimes - sexual offending against children. In *Cybercrime: A review of the evidence*. Research Report 75. pp.1- 25. Retrieved

from:https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/246754/horr75-chap3.pdf; <https://www.gov.uk/government/publications/cyber-crime-a-review-of-the-evidence>

McNally, A., (2016). "Every picture tells a story". A study of those who gather and accumulate legal and illegal images. PhD, Nottingham Trent University.

NatCen Social Research (January 2018). Behaviour and Characteristics of Perpetrators of Online-facilitated Child Sexual Abuse and Exploitation, Retrieved from: <http://www.natcen.ac.uk/news-media/press-releases/2018/january/new-report-on-online-child-sexual-abuse-identifies-most-at-risk-children/>

Nurse, J. (Aug 30, 2019). Fortnite is setting a dangerous security trend, *The Conversation*. Retrieved from: <http://theconversation.com/fortnite-is-setting-a-dangerous-security-trend-102294>

Office of the Children's eSafety Commissioner & ACMA. (2016, July 20). Are you GO-ing Pokemon crazy? Retrieved from: <https://www.esafety.gov.au/about-the-office/newsroom/blog/are-you-going-pokemon-crazy>

Pierce, R. L. (1984). Child pornography: A hidden dimension of child abuse. *Child abuse & neglect*, 8(4), pp. 483-493.

Rutkin, A. (2016, August 2). Could sex robots and virtual reality treat paedophilia? *New Scientist*. Retrieved from: <https://www.newscientist.com/article/2099607-could-sex-robots-and-virtual-reality-treat-paedophilia/>

Schermer, B. W., Georgieva, I. N., Hof, S., & Koops, B. J. (2016). Legal aspects of sweetie 2.0., Center for Law and Digital Technologies Leiden University, Faculty of Law. Retrieved from: <https://research.tilburguniversity.edu/en/publications/legal-aspects-of-sweetie-20>

Sward, A., Vecna, I., & F. Stonedahl (2018). Data Insertion in Bitcoin's Blockchain. *Ledger*, 3. Retrieved from: DOI 10.5915/LEDGER.2018.101

Svedin C. G. (2012). Victims assistance, Launching Conference on Global Alliance Against Sexual Abuse Online. EU: Brussels. Retrieved from: <https://www.ecpat.org/wp-content/uploads/2016/05/Emerging-Issues-and-Global-Threats-Children-online-2017-1.pdf>

Takahashi, D. (2016, April 13). Naughty America tries to get VR porn just right. *Venturebeat*. Retrieved from: <https://venturebeat.com/2016/04/13/naughty-america-tries-to-get-vr-porn-just-right/>

Taylor, M., G. Holland, & E. Quayle, (2001). 'Typology of paedophile picture collections', *The Police Journal*, Vol 74, pp. 97-107.

Thorn. (2016). The intersection of child sexual exploitation and technology. Retrieved from <https://www.wearethorn.org/child-sexual-exploitation-andtechnology/>

Toulalan, S. (2014). "Is He a Licentious Lewd Sort of a Person?": Constructing the Child Rapist in Early Modern England, *Journal of the History of Sexuality*, Vol. 23, No. 1, pp. 21-52.

Quayle, E., Jonsson, L., Cooper, K., Traynor, J. & Svedin, C. (2018). Children in Identified Sexual Images - Who Are they? Self- and Non-Self-Taken Images in the International Child Sexual Exploitation Image Database 2006-2015. *Child Abuse Review*, 27(3), pp. 223-238.

United Nations Development Plan & ASEAN (2017). ASEAN-China-UNDP Report on Financing the Sustainable Development Goals (SDGs) in ASEAN: Strengthening Integrated National Financing Frameworks to Deliver the 2030 Agenda. Retrieved from: www.asia-pacific.undp.org/.../launched-publication-on-financing-the-SDGs.html

United N Office of Drugs and Crim (UNODC), (2015). *Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children*, UNODC Vienna; Retrieved from: https://www.unodc.org/documents/Cybercrime/Study_on_the_Effects.pdf

Webster, S., Davidson, J., Bifulco, A., Gottschalk, P., Caretti, V. & T. Pham. (2012). European Online Grooming Report. *European Commission*, Safer Internet Plus Programme. pp. 1-152. Retrieved from: https://www.researchgate.net/publication/257941820_European_Online_Grooming_Project_-_Final_Report

WeProtect Global Alliance (2018). Working together to end the sexual exploitation of children online. Global Threat Assessment 2018. Retrieved from: https://static1.squarespace.com/static/5630f48de4b00a75476ecf0a/t/5a83272c8165f5d2a348426d/1518544686414/6.4159_WeProtect+GA+report.pdf

Walsh, W., Wolak, J. & D. Finkelhor (2012). Methodology report – 3rd National Juvenile Online Victimization Study (NJOV3): Prosecution study. September 2012. Retrieved from: http://unh.edu/ccrc/pdf/CV293_NJOV3%20Prosecution%20Study%20Methodology%20Report_1-18-13.pdf

Webb, L., J. Craissati, & S. Keen (2007). 'Characteristics of Internet child pornography offenders: a comparison with child molesters', *Sex Abuse: A Journal of Research and Treatment*, Vol 19, pp. 449-465.

Wittes, B., Poplin, C., Jurecic, Q. & Spera, C. (2016). Sextortion: Cybersecurity, teenagers, and remote sexual assault. Center for Technology at Brookings. Retrieved from: <https://www.brookings.edu/research/sextortion-cybersecurity-teenagers-and-remote-sexual-assault/>

World Health Organisation, (1999). *Report of the consultation on child abuse prevention*, Geneva, World Health Organization, p. 15. Retrieved from: <https://apps.who.int/iris/handle/10665/65900>

Wortley, R. & S. Smallbone, eds., (2006). *Situational prevention of child sexual abuse*, NY: Criminal Justice Press.

Wolak, J., Finkelhor, D., Walsh, W., & L Treitman (2018). Sextortion of minors: characteristics and dynamics. *Journal of Adolescent Health*, 62(1), pp. 72-79.

Wolak, J. (2015). Technology-facilitated organized abuse: An examination of law enforcement arrest cases. *International Journal for Crime, Justice and Social Democracy*, 4(2), pp. 18-33.

Young, K. (2008). 'Understanding sexually deviant online behaviour from an addiction perspective', *International Journal of Cyber Criminology*, Vol 2 (1), pp. 298-307.