# Virtual Global Taskforce
# Online Child Sexual Exploitation: Environmental Scan
# Unclassified Version
# 2019

*The VGT aims to make the Internet a safer place, identify, locate and help children at risk and hold perpetrators appropriately to account.*

*The Report Abuse button on the VGT website is an effective way to report suspicious online behaviour.*

*www.virtualglobaltaskforce.com*

---

## 1. Executive Summary[1]

Key findings are as follows:

- Currently, the largest international threats in the areas of online child sexual exploitation and transnational child sex offending include:
    - o increased support for personal privacy;
    - o increased accessibility to the Internet;
    - o increased production and consumption of child sexual exploitation material; and,
    - o the location of victims and offenders.

[1] The VGT would like to express its gratitude to all agencies of the international community for their cooperation in this assessment. Particular thank you to the countries who joined the Royal Canadian Mounted Police (RCMP - Canada) in the working group - Australia, Europol, and United Kingdom - who provided assistance and guidance in preparing this report.

- The most significant emerging trends observed globally over the last three years include the increase in:
    - self-generated sexually explicit material;
    - anonymization technologies;
    - use of social media applications; and,
    - live-streaming of child sexual abuse.

- The most substantial challenges for law enforcement agencies relate to
    - technology;
    - legislation; and,
    - the social environment.

- While child sexual abuse is not a new phenomenon, the Internet has transformed the threat into a global issue. Although cooperation amongst countries is increasing, there are still many barriers to providing a streamlined global response.

## 2. Introduction

The Virtual Global Taskforce (VGT) is an international alliance of dedicated law enforcement agencies, non-governmental organizations (NGOs) and Industry partners, working together to reduce the global threat from, and vulnerability of children to, online sexual exploitation and abuse and other forms of transnational child sexual offending. Using a 4P strategic framework, the VGT members deliver a program of coordinated international law enforcement activities which:

- PURSUE by disrupting criminal activity;
- PREVENT offenders from committing crime;
- PROTECT children from being victimized and/or revictimized; and,
- PREPARE law enforcement to anticipate and effectively deal with emerging threats and trends.

This Environmental Scan (e-scan) is commissioned by the VGT Board of Management to assist in the identification of the strategic priorities of the VGT for the next three years, and to guide initiatives and projects endorsed by the VGT. This report also allows the VGT to more fully inform global leaders about the nature and future of this crime-type from an international law enforcement perspective.

## Methodology

The findings outlined in this report were informed by responses provided by VGT members and partner agencies to a global survey pertaining to threats, trends and challenges observed over the last three years on the topics of online child sexual exploitation (OCSE) and transnational child sexual offending (Section 3). Some questions had a list of answers[2] provided where respondents were asked to select the top three best responses for their country. Space was also provided below each question for other answers, and to offer additional explanation. In addition, the responses were complemented by recent literature and other specialized sources (2015-2018) submitted by VGT partners (i.e. reports published by the End Child Prostitution and Trafficking (ECPAT) International, International Centre for Missing and Exploited Children (ICMEC), Internet Watch Foundation (IWF), Europol, NetClean, WeProtect Global Alliance, etc.). More details on these reports can be found in the references section.

To ensure proper understanding of the terminology utilized in the survey, OCSE was defined as offences related to possessing, distributing, producing and accessing child pornography[3][4], online grooming and luring. In addition, transnational child sexual offending was defined as sex offenders travelling abroad (for example, short-term visitors or longer-term visitors who are volunteers/employees in the travel industry, education sector or within non-governmental organizations) or using live-streaming capabilities to sexually exploit and abuse children.

In addition to these topics, survey respondents were asked to identify areas in need of further research and assessment (Section 4), as well as what they would like to see the VGT accomplish in the next three years (Section 5). A total of 48 responses were provided to the above-mentioned survey from nine (9) VGT law enforcement member countries[5]

[2] The answers were informed by recent literature on the threat and trends in the area of online child sexual exploitation.

[3] Although 'child pornography' remains the term used within the legal context across a number of countries (for example, refer to s.163.1 of the *Criminal Code* of Canada), child sexual abuse material or child sexual exploitation material is considered more appropriate terminology as it accurately reflects the reality of the material (ECPAT International, 2016; refer to pp. 38-40).

[4] Various definitions exist internationally for child pornography. These country-specific variances are to be considered when reviewing the findings of this report.

[5] Surveys were initially disseminated to VGT member agencies, and then shared more broadly with their domestic partner agencies.

(Australia[6], Canada[7], Netherlands[8], New Zealand[9], South Korea[10], United Kingdom[11] and United States[12]) and organizations (Europol; Interpol[13]; two NGOs[14]; and, one Industry member[15][16].

# 3. Findings

## 3.1 International Threats

This section establishes the current four[17] largest international threats in the area of OCSE and transnational child sexual offending, as indicated by survey respondents. For the purpose of this environmental scan, the term threat is to be understood as a negative event that can increase the risk of victimization for this crime-type. The responses have been supplemented by information originating from academic literature and other specialized sources.

[6] A total of 7 responses were received from the Australian Federal Police (a VGT member agency), Queensland Police Service Taskforce Argos, Office of the eSafety Commissioner, Department of Home Affairs National Security and Law Enforcement Policy Division, South Australia Police, Tasmania Police and Western Australia Police. The responses were combined into one comprehensive response to ensure equal representation amongst the other participating countries.

[7] A total of 26 law enforcement responses were received from Internet Child Exploitation units (of various police agencies) across Canada, including the RCMP (a VGT member agency), and were combined into one comprehensive response to ensure equal representation amongst the other participating countries.

[8] Two responses were received from the Netherlands (Dutch National Police) and were combined into one comprehensive response to ensure equal representation amongst the other participating countries.

[9] Online Child Exploitation Across New Zealand (OCEANZ) of the New Zealand National Police.

[10] Korean National Police Agency.

[11] National Crime Agency.

[12] Department of Homeland Security (Homeland Security Investigations).

[13] A total of five responses were received from Interpol and were combined into one comprehensive response to ensure equal representation amongst the other participating countries.

[14] International Justice Mission and National Children's Advocacy Center in the United States.

[15] Web-IQ, located in the Netherlands.

[16] For analysis and comparison purposes, responses from Industry and NGOs were grouped together to form a "non-law enforcement" group.

[17] The very subjective, diverse approach of respondents, which is believed to reflect investigative priorities of individual law enforcement agencies, made the analysis of this survey quite challenging. Thus, the top four threats were identified based on frequency of appearance in the survey responses and are not necessarily ranked in order of importance.

### 3.1.A. Support for personal privacy

When technology, including encryption, is used for legitimate transactions and online activities, personal privacy is to be respected and protected. However, when these technologies are used by offenders to commit crime, the support for personal privacy can quickly become problematic, especially for law enforcement. Seven out of nine VGT law enforcement member countries/organizations identified society's increased support for personal privacy - as opposed to law enforcement having access to basic subscriber information (BSI) - as a main threat to OCSE and transnational child sexual offending investigations[18]. This threat was also identified by one of three non-law enforcement participants.

Closely linked to privacy, more offenders are using anonymizing technologies such as TOR[19] as well as VPNs[20] to commit sexual offences against children online. This is most likely due to the privacy features offered by these services that are perceived by some to be offering "protection from prosecution" according to one law enforcement respondent. The subsequent belief that offenders are protected and the resulting feeling of impunity has enabled diversification of methods to sexually exploit children, resulting in new and persistent threats. Evolving case law related to basic subscriber information greatly hinders the ability to prioritize files where children are at risk. For example, the *R. v. Spencer* decision in Canada now requires law enforcement to submit a judicial authorization signed by a judge to Internet Service Providers (ISPs) to obtain BSI, as opposed to a simple law enforcement request (i.e. email). This process significantly slows down the investigation process since more steps are required to identify the suspect using these services that affect law enforcement's ability to respond in a timely manner and safeguard children.

Due to privacy regulations, the monitoring of online platforms for child sexual exploitation material (CSEM) is also challenging, increasing the threat of OCSE. Ensuring that the services they provide to the public are free of CSEM requires a commitment and an investment by Industry. Many countries make a legal requirement of such platforms

[18] Specifically, the General Data Protection Regulation (GDPR) is a regulation on data protection and privacy for all individuals within the European Union and the European Economic Area which prevents law enforcement from gaining access to some data they require to effectively investigate.
[19] The Onion Router (TOR) is a free software for enabling anonymous communication online.
[20] A Virtual Private Network (VPN) is a private network and enables users to send and receive data across shared or public networks as if their devices were directly connected to the private network.

to prevent or take down CSEM when it is detected. The ability of Industry to comply with this requirement varies from one company to another due to limitations like capacity or capability.

In addition, storing this material is also illegal (e.g. keeping evidence for a long period of time after reporting it to law enforcement)[21]. Moreover, the introduction of the European ePrivacy Regulation may create complications for European and US companies' use of PhotoDNA, given the draft Regulation's current focus on preventing data-processing without the relevant data-subject's approval. In addition, it was mentioned by law enforcement that privacy laws also prohibit forensic examination as investigators are often unable to examine locked and/or encrypted smart phones due to privacy laws and encryption methods. As such, the heightened focus on the need for online privacy for individuals must be carefully balanced with the rights and protection of the vulnerable, and society at large (WeProtect Global Alliance, 2018, p.30; see also the joint statement from Europol and the European Union Agency for CyberSecurity (ENISA), issued on May 23rd, 2016[22]).

To mitigate this specific threat, survey respondents provided recommendations[23] such as:

- Increasing advocacy for/awareness of the importance of retaining and having access to BSI, evidence on electronic devices as well as monitoring online platforms to successfully pursue offenders and reduce/prevent victimisation and re-victimisation. At the very least, there should be an exception to privacy laws when a child is at imminent risk of harm (sexual, physical, etc.);
    - Engage in discussions within Internet governance to ensure that law enforcement has a voice in changes in policy which might affect access to data.
- Increasing mandatory minimum sentences to deter offenders from committing such offences, and using these technologies in the first place (the consequences for their actions are currently disproportionate to the harm inflicted upon their victims)[24];

[21] Albeit this could probably be overcome by companies being explicit in their terms and conditions about their proactive prevention of CSEM.

[22] https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/on-lawful-criminal-investigation-that-respects-21st-century-data-protection

[23] Please note that not all participating law enforcement agencies agreed on these recommendations. The list combines individual recommendations provided by the agencies.

[24] To note: law enforcement agencies, as well as experts in this area, differ on the effectiveness of deterrence.

- Enforcing an even application of the mutual legal assistance treaty (MLAT)[25] process;
- Offering an electronic submission of the production order to streamline the process of accessing BSI; and,
- Further lobbying international political groups and governments to require VPN companies to store information about their users.

Some of these recommendations could be actioned in collaboration with the WeProtect Global Alliance whose Model National Response to Tackling Child Sexual Abuse and Exploitation helps countries establish and develop coordinated national responses to OCSE. Using the Model, countries can evaluate their current response, identify gaps and prioritize national efforts to address them. It is important to recognize that engagement with Internet governance bodies is already taking place at an operational level, for example through Europol and the European Multidisciplinary Platform Against Criminal Threats (EMPACT) Cyber child sexual exploitation action plans.

### 3.1.B. Accessibility to the Internet

The greater accessibility to the Internet was mentioned by six of nine VGT law enforcement member countries/organizations and one of three non-law enforcement members as the main cause for the increased exposure to the threat. The Internet has become readily accessible on various devices (i.e. smart phones, laptops, and computers), and at decreasing costs, greatly increasing the number of people with access to a plethora of websites and social media applications, particularly in Africa, South East Asia, South America (WeProtect Global Alliance, 2018) and the Pacific Islands (New Zealand, 2017). WeProtect Global Alliance (2018) anticipates there will be over 5 billion smart phone users in 2019, and currently one third of the world's population is connected through social media platforms, including 800 million children. Although the Internet is considered indispensable for entertainment, sharing media, and communication, various Internet technologies and platforms are also being used by child sex offenders to target vulnerable children and sexually exploit them.

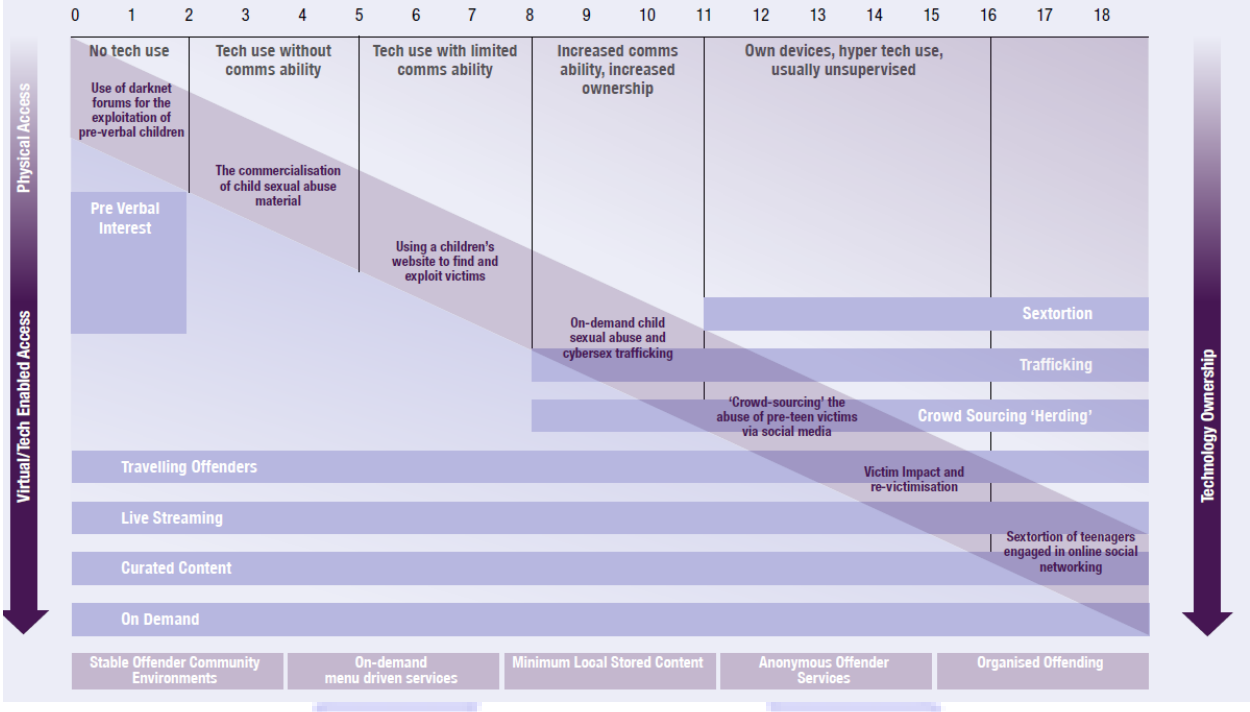
Since children are more connected than ever, the virtual realm represents a substantial threat as it provides child sex offenders with almost unlimited access to children for sexual exploitation purposes. The Internet also provides a place in which offenders can find other like-minded individuals with whom they can share advice on how to abuse children and

[25] An MLAT is an agreement between two or more countries for the purpose of gathering and exchanging information relevant to an investigation.

evade law enforcement, discuss which global locations are most convenient for abuse opportunities, as well as to access and distribute CSEM (ECPAT International & INTERPOL, 2018; Europol, 2017a; Europol, 2018; WeProtect Global Alliance, 2018).

Adding to this threat is parents' lack of supervision and knowledge of children's online activities. Children now have access to electronic devices at a very young age; however, they may not yet have the maturity, tools and skills to differentiate between online friendships and relationships, and online sexual exploitation. With the constant proliferation of new websites and apps promoting anonymity and privacy, and the availability of electronic devices, children and youth are increasingly more prone to self-exploitation, which puts them at risk of online grooming, luring and sextortion.

In the 2018 Global Threat Assessment, WeProtect Global Alliance published a table showing the intersection between victim, offender and technology. The findings suggest that as a child progresses through childhood, they become susceptible to a range of different threats.




The graph demonstrates that as we become more connected and gain greater access to the Internet, law enforcement is seeing a more permissive environment online for international offender behaviour, grooming and sextortion (WeProtect Global Alliance, 2018).

A final growing concern with youth's increased access to the Internet, is the desensitisation to sexual and violent content (NSPCC, 2016; as cited in WeProtect Global

Alliance, 2018). "Numerous studies of teenagers in western countries show that viewing such content online is prevalent, and has a negative impact on the way that teenagers interact, what they expect, and what they deem age-appropriate sexual behaviour" (WeProtect Global Alliance, 2018, p.17).

A law enforcement survey respondent indicated that the lines between legal and illegal material are often blurred. More pornography consumers are becoming interested in extreme material which can contribute to the demand for CSEM (CPCMEC/BSB, 2015).

To combat this threat, survey respondents suggested education and awareness campaigns (which include prevention strategies) for both young children (continued throughout school years) as well as parents, carers/guardians and professionals. There is a need to promote a healthy balance between utilizing the Internet for all its benefits, and ensuring youth's online safety. Safe online behaviours should be encouraged, in addition to restricting youth access to the Internet.

### 3.1.C. Increased production and consumption of child sexual exploitation material

As a result of the increased accessibility to the Internet and growing volume of electronic devices such as smart phones, most participating VGT law enforcement member countries/organizations (7/9) recognized the increased production and consumption of CSEM, at a very low cost, as a major current threat to investigations. This growing threat was also identified by numerous other agencies and organizations. A few of those statistics are provided below.

- 70% of the Global Alliance Threat Assessment respondents (Global Alliance against Child Sexual Abuse Online [Global Alliance], 2016) identified an increase in the volume of CSEM online;
- The United States' National Center for Missing and Exploited Children (NCMEC)[26] received over 18.4 million reports in 2018, a momentous increase from the 1.1 million reports received in 2014;
- The RCMP's National Child Exploitation Crime Centre (NCECC) has observed a 566% increase in the number of incoming OCSE reports received from 2015 to 2018;
- WeProtect Global Alliance (2018) reported a 57% increase in domains showing images of child sexual activity;

[26] NCMEC is an NGO whose mission is to help find missing children, reduce child sexual exploitation, and prevent child victimization. Visit www.missingkids.com for more information.

- In 2018, IWF noted a 32% increase from the previous year in the number of processed reports confirmed as containing CSEM, with an increasing number of webpages being hosted in Europe (from 41% to 79%), rather than North America (from 57% to 16%) – a progressing shift since 2015. Moreover, 3,899 domain names worldwide were used to create links to these URLs[27], representing a 61% increase from 2016. Furthermore in 2018, every five (5) minutes IWF assessed a webpage that shows a child being sexually abused (Internet Watch Foundation, 2018);
- The Pacific Transnational Crime Coordination Centre (PTCCC) has reported an increase in referrals regarding child sexual exploitation (New Zealand Police, 2017);
- Project Arachnid[28] currently identifies over 80,000 unique images of child sexual abuse on the Internet per month (WeProtect Global Alliance, 2018); and,
- In 2017/18, the Canadian Centre for Child Protection[29] (C3P) processed 139,897 CSE reports, a 248% increase in reports over 2016/17 (C3P, 2018).

Both supply and demand for CSEM are increasing simultaneously as offenders have easy and constant access to the Internet. In a global survey, 81% of responding countries indicated that the number of online offenders has increased, 97% of responding countries asserted that the number of images per offender had increased, while 93% indicated that the number of images in circulation has risen (Global Alliance, 2016). These increases were mainly attributed to a growing ability to store content online (i.e. cloud-storage and links provided to a large number of people with relative ease), increased access to the Internet from various types of electronic devices as well as an increase in public reporting of CSEM online. In addition, one law enforcement respondent noted that increased communication between child sex offenders online has increased the pressure to produce new CSEM, with this incitement resulting in an escalation of offending. Many individuals would be content with the material readily available online; however, when communicating with others and being part of offender forums, especially on the dark net, the production of "never-seen before" material has become a requirement, further proliferating the supply and demand, in addition to the victimization of children[30]. In that regard, few law enforcement

[27] A Uniform Resource Locator (URL) is the specific location where a file is saved online (Internet Watch Foundation, 2017).
[28] Project Arachnid is an automated tool created by C3P which searches the Internet for any child sexual exploitation material.
[29] The Canadian Centre for Child Protection is a national charity dedicated to the personal safety of children. Their goal is to reduce the sexual abuse and exploitation of children, assist in the location of missing children, and prevent child victimization. Refer to https://www.protectchildren.ca for more information.
[30] Law enforcement is seeing an absolute requirement for offenders to regularly post first generation images to gain access to these sites. They often contain the worst of the most heinous abuse imagery.

respondents found the removal of CSEM via takedown request/notice by INHOPE, C3P and other hotlines as an effective way of disrupting access to abuse material.

A number of organizations can offer figures and data to inform estimations of the growth, nature and scale of OCSE. However, these numbers only represent a fraction of offences being perpetrated every year as many offenders remain undetected and victims remain unidentified. The findings in this e-scan demonstrate that the threat to children posed by online sexual offenders is increasing. Survey respondents indicated that they are currently unable to adequately handle case file volumes and that more work is required to better understand the volume of this crime-type on a global scale, and find solutions to break the cycle of supply and demand of CSEM online. Law enforcement respondents recommended further collaborating with Industry to pursue efforts to reduce the overall availability of CSEM online. Law enforcement should also consider their triage processes and feedback to Industry.

### 3.1.D. Location of victims and offenders

From a global perspective, the location of victims and offenders was equally noted as a substantial threat to OCSE by six of nine participating VGT law enforcement member countries/organizations and two of three non-law enforcement partners. With the increased accessibility to the Internet, offenders now have the ability to sexually exploit children who are residing in other jurisdictions and even other countries. This has resulted in an increase in the virtual production of CSEM, putting a larger portion of the global youth population at risk. A common misconception is the fact that victims of online CSE largely reside in developing countries; while in fact, reports from law enforcement indicate that just as many victims reside in North America and Europe, as those victims who have been identified as residing in Latin America, Africa and the Middle East (WeProtect Global Alliance, 2018). It is important to note, however, that this crime-type exists worldwide and increased detection capacities and capabilities may skew the perception of where occurrences are most prevalent (WeProtect Global Alliance, 2018).

IWF (2018) found that 87% of all child sexual abuse URLs identified by IWF in 2018 were hosted in five countries: Netherlands (47%), United States (12%), Russia (11%), Slovak Republic (11%) and France (6%) (IWF, 2018).

Online child sexual exploitation is facilitated by recent technological developments that enable direct communication between offenders and victims, as well as offenders and other offenders, from all over the world. Widespread Internet access has created a

favourable environment for the sexual exploitation of children located in all parts of the world. Consequently, law enforcement survey respondents indicated how international cooperation to combat this crime-type is essential, but can be challenging as different countries have differing priorities, while some lack investigational capacities and capabilities, and have inadequate legislation to protect child victims of sexual abuse, particularly online.

As a recommendation to these established obstacles, some survey respondents suggested monitoring the latest developments in victim identification techniques and technology, and actively promoting the cooperation of law enforcement on this issue.

### 3.1.E. Non-law enforcement-identified threat

As opposed to the responses provided by VGT law enforcement member countries/organizations, non-law enforcement members identified an increase in the use of peer-to-peer (P2P) file sharing as a substantial threat (2/3). In fact, the threat posed by P2P has been highlighted recently by Europol in the Internet Organised Crime Threat Assessment (IOCTA) in 2017 and 2018, as well as in the Serious and Organised Crime Threat Assessment (SOCTA) in 2017.

More generally, the VGT sees an enhanced role for Industry partners by encouraging companies to move from a reactive position of making referrals to law enforcement, to a proactive position of preventing offending from happening.

## 3.2. International Trends

This section establishes the top three emerging trends that survey respondents have noticed when investigating OCSE offences over the past three years. Additional trends identified in other specialized sources of information were also added. In this context, a trend is defined as a general development in the way offenders and victims of OCSE are behaving.

### 3.2.A. Self-generated sexually explicit material

VGT law enforcement member countries/organizations (5/9), and non-law enforcement members (2/3) who participated in the survey noted an increase in the number of children

and youth producing self-generated sexually explicit material. Law enforcement and experts in child sexual exploitation from around the globe have also noted this emerging trend (ECPAT International & INTERPOL, 2018; Europol, 2017c; Europol, 2018; IWF, 2017; NetClean, 2018; New Zealand Police, 2017), including those surveyed for the Global Alliance Threat Assessment (2016) questionnaire where 84% of respondents reported an increase in those cases over the past five years. This emerging trend is particularly interesting since law enforcement agencies surveyed in the 2012 VGT e-scan noted that there was only limited evidence that self-generated sexually explicit material was starting to be seen in CSEM collections.

Once children and youth begin to manage their own Internet use, the ways in which they can be exploited increase (WeProtect Global Alliance, 2018). Youth may self-generate material to be shared with peers (i.e. voluntarily self-produced, innocent); however, this material may also be sexually explicit in nature and end up being shared with another person without the youth's consent, such as adult strangers online, and subsequently used for manipulation purposes (Europol 2017; NetClean, 2018). Law enforcement has observed a trend where sexting[31] is becoming a normal and almost encouraged practice among youth, contributing to the proliferation of CSEM. As noted by a VGT survey respondent, children are self-producing more material now for online gifts, real gifts, money or even for the promotion of their own self-esteem. Many do not understand the numerous consequences related to the self-production of such material.

A common outcome to youth producing self-exploitation material is sextortion (ECPAT International & INTERPOL, 2018; Europol, 2017a; Europol 2017c; Global Alliance, 2016; New Zealand Police, 2017). Sextortion is defined as "the blackmailing of a person with the help of self-generated images of that person in order to extort sexual favours, money, or other benefits from him/her under the threat of sharing the material beyond the consent of the depicted person (e.g. posting images on social media)" (ECPAT International, 2016: pg. 52). As more and more children have access to the Internet and countless social media platforms, numerous agencies and organizations have reported a rise in the number of cases involving sextortion. A report produced by the Brookings Institution in 2016 noted that offenders used sextortion in 91% of cases involving minors (as cited in ICMEC, 2018a). The United States Department of Justice's National Strategy for Child Exploitation and Prevention and Interdiction report said that sextortion was one of the largest growing threats towards children online (ICMEC, 2018a).

[31] Sexting is the act of sending, receiving or forwarding sexually explicit messages or images, primarily between mobile phones, of oneself to others (dictionary.com, 2019).

Typically, sextortion victims are older minors and female. The majority of sextortion victims are between the ages of 10 and 17 years of age (ICMEC, 2018a). A study by NCMEC found that in 78% of reported sextortion cases, the victim was female between 8 and 17 years of age (as cited in ICMEC, 2018a). Although sextortion victims can also be adults, the Brookings Institution study found that in 71% of the cases analyzed, a minor was victimized (as cited in ICMEC, 2018a). Additionally, recent investigations have uncovered the existence of organized sextortion groups. These groups often located abroad, use call center-like operations in order to communicate with hundreds of potential victims at once (ICMEC, 2018a). Individuals from these organized crime groups have contacted and victimized children as young as 14 years of age (ICMEC, 2018a).

Further, 70% of responding countries to the Global Alliance Threat Assessment questionnaire noted an increase in the number of cases where the offender used extortion, blackmail, threats, and other forms of coercion to force their victims to produce sexually explicit material (Global Alliance, 2016). There is also an emerging indication that more women are perpetrators of sextortion in order to extort sexual favours, money, or other benefits from their victim(s) (ECPAT International, 2017). Child sex offenders are using the Internet to gain children's trust by posing as someone of a similar age, or developing a friendship or relationship, before persuading them to share sexually explicit images or videos. Once this material is sent, the offender threatens to share the material with the child's friends and family if s/he does not continue to comply with his/her demands for additional content, which is, oftentimes increasingly more explicit in nature (Europol, 2017a; Europol, 2017c; WeProtect Global Alliance, 2018). In addition to its criminal nature, sextortion is particularly concerning because of the profound psychological impact on the victims. The continuous manipulation and threat of being exposed is very distressing. Negative psychological impacts of sextortion include feelings of low self-esteem, withdrawal, worthlessness, anger and guilt. In some cases, victims have engaged in self-harm and/or attempted suicide[32] (ICMEC, 2018a).

Law enforcement considers these investigations considerably challenging since it is nearly impossible to determine whether the images/videos were self-generated by a consenting youth or generated after being coerced or sextorted (ECPAT International & INTERPOL, 2018; Europol, 2017c). As one survey respondent illustrated, once the images/videos are distributed online, it becomes extremely difficult to remove them from the virtual realm because they are often copied and distributed repeatedly. This results in the incessant re-

[32] Cybertip.ca in Canada offers an online mechanism where youth can submit anonymous requests to have any image or video that was uploaded or shared online without their consent, removed from the Internet. This online tool has helped numerous children report the abuse and have the image/video removed before being further distributed.

victimization of children. To reduce these incidents, C3P has created a platform (Cybertip.ca) where children and youth can submit a request to have any image/video posted and distributed online, without their consent, removed from the Internet. This initiative has not only reduced the number of re-victimized children but has also helped victims regain some control of their images.

As a recommendation to reduce the proliferation of self-generated sexually explicit material, law enforcement survey respondents suggested developing better prevention and education programs for children and youth, including awareness campaigns for parents and legal guardians on the topics of online safety, sexting and sextortion. Efforts in this area are in progress with the VGT website now hosting links to educational resources for each member country and agency, where generic advice is also provided to advise on how to develop one's own resources.

### 3.2.B. Increased use of anonymization

As previously stated, in section 3.1, an increasing number of offenders are now using anonymization technologies to hide their identities and conceal online activities in the hope of reducing the risk of detection. Notably, six surveyed VGT law enforcement member countries/organizations and one non-law enforcement partner indicated that anonymity tools are now readily available to the general public, making it easier for the less technologically-inclined offenders to sexually exploit children online with little risk of being caught. Similarly, 84% of the countries who responded to the WeProtect Global Alliance Threat Assessment (2018) questionnaire recognized the increased use of anonymization technology as the largest emerging trend involving child pornography and the enticement of children[33]. This trend was also identified in the 2012 VGT e-scan but has since progressed and further proliferated, specifically OCSE cases (Europol, 2017a; Europol, 2017b; Europol, 2018).

Offenders are becoming more organized and creative with the ways in which they hide their activities and identities (Netclean, 2018). Particularly, 45.6% of the NetClean (2018) survey respondents noted an increase in the number of organized forums and groups of offenders online in the past three years. Anonymization technologies, which are generally legal to use worldwide, are often shared among offenders who are known to teach each other on how to become anonymous online (Europol, 2018). For instance, several

[33] The term "enticement of children" was defined in the threat questionnaire as the use of digital technology, including the Internet and mobile phones, to persuade, induce, entice, and/or coerce an individual who is under the age of 18 and located in another country to engage in illegal sexual activity (WeProtect Global Alliance, 2018).

responding countries to the Global Alliance Threat Assessment questionnaire indicated how offenders are more commonly educating each other on how to use private chats, email, Internet voice and video chat software, forums and anonymization software (Global Alliance, 2016). These technologies may also be used to avoid country-specific Internet content blocking capabilities. Furthermore, many communication service providers now offer anonymization and encryption tools as a default capability. For example, WeProtect Global Alliance (2018) indicated how the increased news coverage regarding government surveillance has invigorated the development of secure and anonymous services such as VPNs that acquire 350,000 new users every day, exchanging 15 billion messages per day.

Again, law enforcement survey respondents recommended the development of technologies to assist in the de-anonymization of offenders online including through further engagement with Industry partners.

### More offenders on the dark net[34]

The recent shift toward a strong need for online anonymity has also pushed offenders to be more actively present on the dark net (Europol, 2018). Notably, three of nine VGT law enforcement member countries/organizations and one of three non-law enforcement members who participated in the VGT survey observed an increase in investigations occurring on the dark net. These tend to require more resources as they are more complex, especially when they involve international partner agencies. The WeProtect Global Alliance (2018) found that hidden services[35] on the dark net are dedicated to various aspects of child sexual offending. For example, some services are particularly being used by offenders to produce and distribute sexual abuse material involving infants/toddlers (also described as pre-verbal children) who are unable to self-report their abuse. One such website has over 18,000 registered members who regularly meet online and discuss their preference for this age group. Moreover, a forum dedicated to discussing the abuse of children has exceeded 23 million hits[36] while on another dark net site, each user uploaded one 3 minute video or two images each month as membership payment. Similarly, of the 85 newly-identified hidden services or dark net websites assessed by the IWF in 2018, 40 (47%) of them were deemed "commercial" – offering

[34] Dark web and dark net are often used interchangeably. However, it is believed that dark net is more accurate terminology as it is a deliberately un-linked set of hidden services and resources, as opposed to an html based web of linked sites.

[35] Hidden services are websites that are hosted within a proxy network, which means their location cannot be traced (IWF, 2017).

[36] Hits refer to webpages that are viewed by individuals or the number of files downloaded from a website.

CSEM for sale – as compared to 30% of hidden services assessed in 2017 (IWF, 2018). However, a decline in webpages containing commercial CSEM[37] has been observed from 2015 (21%) to 2018 (7%) which could be due in part to offenders increasingly using disguised websites instead (IWF, 2018). This hypothesis is supported by the IWF (2017) that saw an 86% increase in the use of disguised websites defined as websites where the CSEM is only revealed to someone who has followed a pre-set digital pathway (specific links) leading to the site. Anyone else accessing the website directly through a browser would be shown legal content.

The dark net is an overlay network accessed only with specific software, configurations or authorisation, often using non-standard communication protocols and protective measures. For this reason, dark net sites are appealing to child sex offenders since they are relatively easy to operate and access. This ensures stability within the offender online community, allowing for more material to be created, more members to be added and more victims to be abused (Europol, 2018). For instance, dark net and TOR usage seems to be continually growing, from an initial user base of just under one million in 2013, to over four million users at the start of 2018 (WeProtect Global Alliance, 2018). Further, the NCA assesses there are 2.88 million global registered users across the ten worst child sexual abuse and exploitation dark web sites. More alarming is the potential connection between secure online networks of offenders and contact sexual offending against children. A study conducted in Australia found a possible escalation from passive participation to the production of CSEM and finally to contact sexual offending against children when the offenders were involved in networking (Krone & Smith, 2017). In addition, an emerging trend has been observed by law enforcement whereby offenders are required to produce new CSEM as a means to gain access to these exclusive offender networks on the dark net. Despite the prevalence of this trend, more extensive research is needed to statistically corroborate this correlation (Krone & Smith, 2017).

### 3.2.C. Use of social media applications

Although offenders may be using the dark net and hidden platforms to sexually offend against children, four of nine surveyed VGT law enforcement member countries/organizations and one of three non-law enforcement members have noted the proliferation in the use of social media applications to commit these offences on the open web over the past three years. Youth, especially teenagers, are heavily active on social

[37] Commercial child sexual abuse material is defined as material produced or being used for the purposes of financial gain by the distributor (IWF, 2017).

media applications putting them at risk of online sexual exploitation (WeProtect Global Alliance, 2018). The UK National Crime Agency (NCA) Child Exploitation Online Protection (CEOP) found that offenders tend to approach victims on popular social media applications and websites before inviting them to join a more private messaging platform, often with video chat capabilities, to engage in sexualised conversations. Social media applications are commonly used tools where fake profiles are created by offenders to target a large number of victims at once (Europol, 2017c; WeProtect Global Alliance, 2018).

Children as young as one year old are beginning to use tablets and smartphones. Supervision and frequency of access to the Internet differ significantly depending on families across cultures. This new and emerging trend increases the opportunities for offenders to interact with and sexually exploit children starting at a very young age (WeProtect Global Alliance, 2018). As such, education and awareness of social media risks are key in the prevention of online offending.

### 3.2.D. Live streaming

In the 2012 VGT e-scan, live-streaming of child sexual abuse was established as a new reality, a methodology increasingly used by offenders to sexually exploit children online. Live-streaming involves the participation of a child - by definition, under coercion – in real or simulated sexual activities, alone or with other children or adults, that are transmitted ('streamed') live on the Internet (ECPAT International, 2017). Not only does live video streaming remains a current means to sexually exploit children online (Europol, 2018), but it is expected to grow 15x between 2016 and 2021 and account for 13% of Internet video traffic by 2021 (as cited in WeProtect Global Alliance, 2018). The increased availability of a widely used communication technology like live streaming unfortunately also means that child sex offenders are able to record and stream the sexual abuse of children in real time, from virtually anywhere in the world, to anyone interested in this type of material. Particularly, VGT law enforcement member countries/organizations surveyed (3/9), as well as non-law enforcement members (2/3) noticed an increase in the use of this technology to exploit children, which has been predominantly facilitated by the spread of 4G[38] technology in developing countries (VGT, 2018). In addition, 19 of 33 responding countries to the Global Alliance Threat Assessment questionnaire not only investigated the live transmission of child sexual abuse but 16 of them indicated that the number of such cases increased over the past five years (Global Alliance, 2016). This is likely due to

[38] 4G is the fourth generation of broadband cellular network technology which provides advanced capabilities for mobile devices.

the number of Voice over Internet Protocol[39] (VOIP) platforms, as well as the continued increase in sophistication of mobile digital devices (NetClean, 2018).

Child sex offenders are now able to pay for and direct the live sexual abuse of children while hidden in private homes and Internet cafes without having to leave their own homes (Europol, 2017a; Europol, 2018; WeProtect Global Alliance, 2018). As such, overseas perpetrators can request certain sexual acts to take place in advance of the abuse, or while its underway (ECPAT International, 2017). Particularly, several (57%) responding countries to the Global Alliance Threat Assessment questionnaire reported that such cases have increased over the past five years (Global Alliance, 2016). The sexual activities streamed online may also be recorded, either by the perpetrator abroad or the facilitator at the location of the abuse, and then disseminated online, substantially adding to the volume of CSEM available on the web (ECPAT International, 2017). The cost to produce and watch live streaming of child sexual abuse is relatively low[40], further encouraging offenders to access this kind of performance frequently (ECPAT International, 2017). Moreover, developments of alternative payment systems such as pay-as-you-go also facilitate and embolden the growth of child sexual abuse live streaming (Europol, 2016). In some instances, the use of live-streaming was found to be a precursor to transnational child sexual offending (Europol, 2017a; WeProtect Global Alliance, 2018). Via the Internet, child sex offenders are able to communicate with individuals around the world who are live-streaming the sexual abuse of children, and arrange travel specifically to engage in sexually explicit conduct with the victims. Trends in this area have diversified over the last few years – popular countries of destination and offenders' countries of origin are constantly changing. That being said, online communities remain the preferred environments for offenders looking to sexually abuse children, discuss vulnerability factors and establish which countries should be targeted (WeProtect Global Alliance, 2018).

[39] VOIP is a methodology and group of technologies for the delivery of voice communications and multimedia sessions over the Internet.

[40] Reportedly, the price for each single show varies depending on its length, the number and age of children, and the sexual acts that they perform. Usually the amount ranges between 500 and 2000 Philippine Pesos (currently equivalent to $10-40 USD) (ECPAT International, 2017).

### 3.2.E. Victim Demographics

An analysis of data available through the International Child Sexual Exploitation (ICSE)[41] database revealed that 64.8% of unidentified CSEM depicted female children, 31.1% depicted male children and 4.1% both male and female victims[42]. When boys were depicted in the abuse, it was more likely to be severe or involve paraphilic themes (i.e. bestiality, sadism, humiliation, necrophilia, etc.) (ECPAT International & INTERPOL, 2018). Congruently, IWF (2018) found that 78% of victims were females, 17% males and 4% both sexes. The latter is also consistent with the statistics reported by INHOPE, where 80% of victims were females, 17% were males and 3% both sexes (INHOPE, 2019). Thus, these findings suggest the need for a closer look at victim demographics, as victims are often assumed to be only female. Recent statistics show a possible link between the age of the victim and the severity of the abuse. The younger the victims, the more likely it is that the abuse will be severe and involve an additional paraphilic theme (ECPAT International & INTERPOL, 2018). Paraphilia is often comorbid with other sexual, mood, and personality disorders, characteristic of prolific offenders (Seto, Kingston & Bourget, 2014). Notably, IWF (2018) found that 35% of the CSEM analyzed in 2018 with children appearing to be under the age of 10 was deemed category A[43] (which includes rape and torture), as compared to 16% of the imagery showing children aged 11-17.

Although an increase in self-generated sexually explicit material by pubescent children has been observed over the past three years, pre-pubescent and young children still comprise the majority of the victims depicted in CSEM available online (Europol, 2017a; Europol, 2018). Of the unidentified victims depicted in the analyzed material on the ICSE database, 56.2% were pre-pubescent, 4.3% were infants and toddlers, and 14.1% of the material featured children in multiple age categories (ECPAT International & INTERPOL,

[41] ICSE is a specialised tool for use by certified law enforcement officers and other personnel who investigate CSEM. The main purposes of the database are to facilitate the process of identification of child victims of sexual abuse and to minimise duplication of efforts by law enforcement agencies (ECPAT International & INTERPOL, 2018).

[42] Caveat: these statistics reflect cases reported to law enforcement and may not reflect the entirety of the CSEM available online.

[43] IWF assesses child sexual abuse material based on UK law, according to the levels in the Sentencing Council's Sexual Offenses Definitive Guidelines. Since April 2014, there have been three levels: Category A is defined as images involving penetrative sexual activity; images involving sexual activity with an animal or sadism; Category B is defined as images involving non-penetrative sexual activity; and, Category C is defined as other indecent images not falling within Categories A or B (https://www.iwf.org.uk/what-we-do/how-we-assess-and-remove-content/laws-and-assessment-levels).

2018). IWF (2018) noted that 40% of children in its reports appeared to be aged 0 to 10 while INHOPE observed that 89% of children in their reports were between 3 and 13 while 9% were between 14 and 17 (INHOPE, 2019). Some trends reveal an increase in CSEM showing young children, supporting the perception that children are starting to be abused at a younger age (NetClean, 2018). However, such a correlation was not noted by the VGT survey respondents and has yet to be proven statistically. Overall, trends show there is a risk of sexual abuse throughout childhood and that children of all ages and sexes can be victims of OCSE.

The ICSE database analysis also revealed that 71.6% of CSEM depicted a single victim which speaks to the secretive nature of child sexual abuse, where silence may be enforced by an offender through grooming and coercion. Cases involving multiple victims (15.7% involving two and 12.7% involving three or more) may indicate intra-familial or peer abuse, or child abuse perpetrated by transnational child sex offenders (ECPAT International & INTERPOL, 2018).

### 3.2.F. Offender Demographics

There is no typical offender profile. Offenders who engage in the sexual exploitation of children online may be of any age, race, sex, occupation, socio-economic status or geographical area (US Department of Justice, 2016). Some offenders only exploit children online, while others also engage in contact sexual offending (referred to as dual offenders). Nevertheless, an ICSE data analysis revealed that 92.7% of identifiable[44] offenders were male, while female offenders were most frequently seen offending with a male offender (5.5%). Interestingly, in those co-offending scenarios, the female offenders were almost always actively involved in the sexual abuse of the child while the male offenders recorded the abuse. In 2% of the cases, the female offenders abused their own children and the women appeared younger (late adolescent, young adulthood) than those depicted abusing a child with a male co-offender. Further, in the 2012 VGT e-scan, an increasing amount of research being conducted on females with a sexual interest in children was recognized. Research reports from CEOP noted an increase in the number of women producing sexually explicit images of children (as cited in Altamura, 2017). While Meter, an Italian organization, noted an increase of approximately 70% in the number of infants being abused by women (as cited in Altamura, 2017). However, since very few women are detected, arrested and convicted for online sexual offences against children, this has fueled the belief that this problem is so uncommon that it is virtually non-existent

[44] The sex of offenders could only be determined in less than half of all analysed CSEM.

(ECPAT International, 2017). These findings support the contention that most OCSE offenders are male, but that further research is required to determine the prevalence rate[45] and better understand the involvement of women in this crime-type. However, there seems to be a general shift in the gender balance in sexual offending. In terms of ethnicity, the ICSE database analysis determined that most offenders were the same ethnicity as their victim(s) (ECPAT International & INTERPOL, 2018).

The link between online and offline sexual exploitation and abuse of children remains uncertain. Notably, during the course of investigating child pornography offences, 70% of responding countries to the Global Alliance Threat Assessment (2018) questionnaire uncovered previously undisclosed child sexual abuse contact offences, and 72% encountered offenders who had a prior conviction for a child sexual abuse contact offence (Global Alliance, 2016). However, the 2017 Australian study did not find a clear transition from online to offline offending (Krone & Smith, 2017).

Thus, with better technological tools, law enforcement could more easily and rapidly filter through the collections and better identify those online offenders also involved in contact sexual offending against children. As indicated by some VGT survey respondents, further research is required to better understand the connection between online and offline sexual offending against children. The demographics of victims and offenders also need further in depth research.

### 3.2.G. Online Child Sexual Exploitation Material Content

Both child sexual exploitation (non-penetrative) and abuse (penetrative) are portrayed in CSEM collections examined over the past few years. Notably, IWF assessed the CSEM reports received in 2018 and found that 23% pertained to sexual activity between adult and children including rape and torture (Category A); 21% pertained to non-penetrative sexual activity (Category B); and 56% pertained to indecent images (Category C). Similarly, an analysis of the ICSE database revealed that 82.4% of the CSEM examined depicted the sexual abuse of children, while 15.2% depicted sexual activity that was exploitative (non-penetrative sexual activity) (ECPAT International & INTERPOL, 2018). Also, C3P (2016), analyzed 43,762 images and videos of child sexual exploitation and found that 50% involved sexual posing, 47.8% involved explicit sexual activity/assaults and 2.23% involved extreme sexual assaults. These findings suggest that offenders tend to collect legal and

[45] Currently prevalence rates ranging from less than 1% of online child sex offenders consuming CSEM up to 30.6% (respondents to online surveys pertaining to sexual solicitation of minors online) (ECPAT International, 2017)

barely legal material (e.g. child posing and nudity) in addition to illegal child sexual abuse material.

Recent law enforcement action in the UK has established a strong link between the possession of childlike sex dolls and possession of child sexual abuse and exploitation images[46]. As reported by two law enforcement respondents to the VGT survey, child-like sex dolls are also a significant emerging trend in terms of the development of new technology to create extremely life-like models of children designed for simulating sexual intercourse. These dolls have functional electronic parts and responses. They are being manufactured overseas upon increasing requests, imported to various countries around the world, and represent a relatively new way in which child sex offenders can use CSEM.

## 3.3 International Challenges

This section outlines the top three challenges of combatting OCSE and transnational child sex offending as identified by both law enforcement and non-law enforcement members who provided responses to the VGT survey. A wide range of challenges were identified by survey respondents, some specific to the responding agency and some broader international challenges. For this reason, the most common challenges were grouped into themes related to technology, legislation and society.

### 3.3.A. Technology

Increasingly, child sexual offending is taking place online and the nature and scale of this crime-type continues to evolve rapidly in line with technology. Based on survey responses, technology-related issues remain the most substantial international challenge for both VGT law enforcement member countries/organizations (8/9) as well as VGT non-law enforcement members (2/3).

The increased use of the dark net, encryption services, anonymization technologies, and peer-to-peer file sharing combined with an increased support for user privacy has

[46] https://www.independent.co.uk/news/uk/crime/child-sex-dolls-uk-paedophiles-seized-borders-jail-prosecutions-a8844406.html#targetText=The%20Crown%20Prosecution%20Service%20(CPS,to%20police%20since%20September%202016

transformed the Internet into a safe environment for offenders (Europol, 2017a; Europol, 2018; WeProtect Global Alliance, 2018).

In addition, employment opportunities offered by the private sector are often more appealing to technically skilled individuals currently working for law enforcement. To mitigate this gap, the NCA runs a "Specials" scheme, encouraging professionals to volunteer and work for the NCA on a part-time basis. Thus, specialized skills and expertise are brought to the NCA. Further, as new platforms, hardware and applications are developed, they require continual assessment, policy amendments and threat evaluation, as well as government response. This being said, encryption is a legitimate tool to maintain privacy and security. Law enforcement should be proportionate in their requests to defeat encryption (in individual cases) and pro-active in their approaches to defeating it through investigative and other techniques, not by weakening it through backdoors (Europol, 2016).

As such, law enforcement increasingly relies on Industry partners to monitor the illegal use of the platforms and services they offer, and report incidents of child sexual exploitation. The assistance and cooperation of Industry partners is also needed to obtain information and evidence necessary to identify the offender and pursue the investigation, which is oftentimes limited. Investing in global technology innovation as well as increasing collaboration between both partners are essential to combatting child sexual exploitation worldwide (WeProtect Global Alliance, 2018).

### 3.3.B. Legislation

More than half of the VGT law enforcement member countries/organizations (5/9) and one of three non-law enforcement members identified substantial challenges to investigations posed by legislation. Each country's legislation pertaining to OCSE and abuse establishes how offenders are penalized and the extent and capacity in which to collaborate with other countries to bring international offenders to justice. However, some countries do not have well-established legislation that criminalizes this crime-type nor do they have dedicated specialized units to enforce legislation currently in place. This lack of adequate legislation also results in sentences that are highly disproportionate to the harm inflicted upon the child victims. Responding agencies to the Global Alliance Threat Assessment questionnaire recognized that child sex offenders are aware of the differences in child sexual exploitation and abuse laws around the world and use the Internet to discuss and exploit them (Global Alliance, 2016).

Data preservation and data retention represent a challenge to investigations due to ISPs[47] data retention policies and practices (New Zealand Police, 2017). A few survey respondents recognized a lack of harmonization of legislation regarding ISPs and noted that many ISPs do not comply with current legislation, or charge law enforcement for access to the information which impedes law enforcement investigations. As such, law enforcement respondents recommended that a consistent global standard be developed for legislation related to OCSE, which equally maintains personal privacy and security. As noted in the WeProtect Global Alliance (2018), the Luxembourg Guidelines provide a mechanism for correct terminology; however, it is not consistently used, making international collaboration complex. To mitigate this challenge, the International Centre for Missing and Exploited Children (ICMEC) developed model legislation in an effort to increase global understanding and enable governments to adopt appropriate legislation to better protect children and combat OCSE (ICMEC, 2018b).

As a recommendation, it was suggested to review the traditional notions of jurisdiction and sovereignty for this crime-type, and understand the issue from a global perspective to enable a comprehensive international response. For instance, the European Directive on Child Sexual Exploitation and Child Pornography establish standards[48] for legislation in this area in Europe that the Member States are required to implement (European Parliament, 2017). The Council of Europe Convention on the Protection of Children from Sexual Exploitation and Abuse requires those states that have ratified it to comply with it in the legislation they adopt and enforce. Influences from key international fora, such as the VGT and WeProtect Global Alliance, are indispensable in the formation of public policy and awareness.

### 3.3.C. Society

Many societal factors exacerbate the global issue of OCSE and transnational child sex offending (WeProtect Global Alliance, 2018). In fact, four of nine VGT law enforcement member countries/organizations and two of three non-law enforcement partners identified the lack of understanding, awareness, and funding of this crime-type as

[47] An ISP is a company or organisation that provides access to the Internet, Internet connectivity and other related services, like hosting websites (IWF, 2017).

[48] The most important improvements introduced by the Directive include more detailed definition of child pornography, increased criminal penalties, the criminalisation of possession and acquisition of online child sexual abuse material, the introduction of a new offence 'grooming' and provisions to remove and/or block websites containing CSEM. The Member States had a two-year deadline for transposition of the Directive, which expired on 18 December 2013.

challenges that interfere with law enforcement's ability to safeguard children as well as identify and apprehend offenders. Many countries cannot keep up with the rapid technological developments nor obtain sufficient funding to enable cutting edge technology to be fully utilized, and consequently, the threat is not prioritized (Europol, 2017a; WeProtect Global Alliance, 2018).

There is a general lack of political and societal awareness and understanding of the issue of OCSE. This results in a lack of proper training and funding to combat this crime-type, as well as a severe lack of long-term support for victims. Notably, accurate and consistent information may be absent, resulting in a perception that the scale of the threat is less than it actually is (WeProtect Global Alliance, 2018). A law enforcement respondent noted an increased normalization and community acceptance of cybercrime, combined with skepticism towards efforts to expand regulatory and investigative powers, which make it difficult to ensure youth safety.

There are cultural differences around the age of consent, marriage, children and sexual behaviour that increase the complexity of an international response. For example, the New Zealand police reported that traditional social beliefs and practices can increase children's vulnerability to exploitation. This is demonstrated in some parts of the Pacific Islands where it is considered culturally acceptable to exploit children for money, transport, food or other material goods. There are some children in certain cultural environments who are willingly provided by their families for financial purposes (New Zealand Police, 2017). Child sex offenders are known to discuss with each other which countries can be visited at a low cost, which countries have police and courts that are corrupt and/or willing to accept bribes, and those countries where the perceived risk of detection is lowest (Global Alliance, 2016). As such, countries should be encouraged to adhere to international treaties such as the UN Convention on the Rights of the Child and the Council of Europe Convention on the Protection of Children from Sexual Exploitation and Abuse.

Moreover, socio-cultural conditions and attitudes such as poverty, inequality, discrimination, access to education, and exclusion influence the vulnerability of children and youth, and the likelihood of sexual offending. For example, countries with strong prejudices against homosexuality deter male victims from reporting any abuse. The same goes for countries where sexual topics are taboo; youth are most vulnerable to abuse and less inclined to report abusive situations (UNICEF, 2016). These factors can create a permissive offending environment coupled with the increased access to the Internet, can increase the supply and demand for CSEM on a global scale (WeProtect Global Alliance, 2018). As such, the nature of the threat is not isolated but rather a problem for the international community. Therefore, countries should remain informed of the risks their

own cultural and societal norms exacerbate. As well, the public should be clearly and responsibly informed to increase civil society engagement.

Finally, self-generated sexually explicit material represents a growing and concerning challenge to law enforcement, especially when not sexually motivated (e.g. shared amongst young people as a joke, or to shock) (Europol, 2017c). As expressed by a law enforcement respondent, these investigations take up a lot of resources and time which could be spent investigating cases of possible hands-on sexual abuse, extortion, etc.. Notwithstanding that, all reports and incidents should be taken seriously and properly assessed before moving forward with a certain intervention strategy. For incidents of deliberate self-exploitation, better education and prevention initiatives facilitated by parents and schools are needed to avoid, if possible, law enforcement involvement[49]. An example of a successful initiative is the #sayno campaign which provides considerable educational resources in all the languages of the EU on the Europol Public Web Site. In Canada, there is also the DontGetSextorted.ca initiative which uses humour to engage teens in a difficult conversation about how to prevent sextortion; they can download naked mole rat gifs and memes as an alternative to sending a nude image of themselves to someone online.

## 4. Further Research Required

Further research is required in the area of OCSE and transnational child sexual offending. VGT survey respondents identified areas of particular interest, as well as specific research questions pertaining to these areas, and these are summarized below[50].

*Health and wellness*

- What are the long term effects of working in OCSE units on the health and wellness of employees?
- What are some mitigation tools/strategies that can assist employees in this area of work?

[49] There is great difficulty in determining the source and circumstances of self-generated material. There could be some very serious offending occurring in these materials, such as grooming and sexual extortion. Therefore, all reports and incidents should be taken seriously and properly assessed.

[50] The VGT will not be conducting research on all of the topics proposed, as some are outside of the VGT mandate and capabilities. However, these could be an opportunity to leverage partners and discuss VGT research priorities for the next three years.

*Victims*

- What social/cultural factors influence children's and youth's vulnerability to this crime-type?
- How many victims of online grooming report offences? Why would children and youth not report an incident of grooming?
- Debunk the idea that viewing and downloading CSEM does not harm the actual victims.
- How can we reduce the number of incidents of youth online self-exploitation?
    - Assess if numerous and continual age-appropriate education about online safety (and age-appropriate resources) reduce the number of self-exploitation incidents.
    - Assess if parents monitoring their children's devices have an impact on reducing the incidents of self-exploitation (versus parents who do not).
- What are the long terms effects of OCSE on victims?
- A study on the situation and context of male child victims depicted in CSEM and the possible underestimation of the victims.

*Online child sex offenders*

- Research online child sex offender demographics
    - Age
    - Sex - specially, a study on female online child sex offenders to better understand their role and involvement in the abuse
    - Occupation
    - Marital Status
- What is the utility and efficacy of prevention and treatment programs for child sex offenders?
    - Better understand the criminal behaviour, sexual deviancy, of online child sex offenders – how can contact offending be prevented?
    - Offer preventative programs where offenders can safely and confidentially seek treatment before offending, or to prevent reoffending, similar to the services offered by the Lucy Faithfull Foundation[51] in the United Kingdom.
- What social/cultural factors influence someone to sexually abuse children?
- What are the pathways into offending?
- Recidivism: what is the relationship between the sentence (years of imprisonment) and the timeframe before an individual reoffends?

[51] The Lucy Faithfull Foundation is a UK-wide charity dedicated solely to preventing child sexual abuse by offering support and a range of services to child sex offenders.

- What is the correlation between online and offline child sexual abuse? Does one lead to the other? Is one the product of the other?
    - The question remains a serious topic of debate which has strong implications for those advocating the seriousness of OCSE offences.
    - How does one offender escalate from online offending to seeking other likeminded individuals, to creating new CSEM?
- Research typologies of online child sex offenders (i.e. CSEM consumers vs luring offenders) – Are there specific subtypes that are more likely to commit contact abuse/reoffend?

  - Accurate diagnosis of genuine prurient interest in children versus pornography addiction that spirals into more exploitative materials.
- Determining which individuals suspected of OCSE offences are at highest risk of contact offending through development and use of a:
    - Prioritization tool based on suspect (i.e. KIRAT)
    - Prioritization tool based on type of CSEM; assess the typologies of CSEM (i.e. bestiality, anime, hentai, fetishes, etc.) and determine which ones represent a higher risk)
- Is there a correlation between voyeurism and paedophilia?

*International cooperation*

- How can capacity and capability training be better coordinated?
- Law enforcement knowledge and use of secure communication channels such as those provided by Europol and INTERPOL should be improved. Similarly, the operational capabilities and support offered by them should be more widely known.
- What are the current capacities (i.e. across agencies) to investigate this crime-type, especially on the dark net?
- How can international production orders (i.e. MLAT) be improved? Could standardized international court orders, like the European Investigation Order (EIO), to access data be created for this crime-type?
    - How could international agencies better share information online pertaining to suspects (i.e. usernames, IP addresses and emails)?

*Scope of the issue*

- What is the scope of the issue in developing countries (i.e. Philippines) and how is the abuse being facilitated?
- How prevalent is on-demand/made-to-order child sexual exploitation material?

- How many individuals download CSEM?
    - Examine the broader scope of the issue and not just the ones that are caught by law enforcement.
- What is the prevalence of transnational child sex offenders and what can be done by frontline police officers?
- What should law enforcement's response be to online vigilante or child abuse activist groups?
- What are the social costs of harm associated with online CSE (i.e. personal and community harm) and how effective are prevention strategies?
- What is the intersection between child trafficking and child sexual abuse, including links to organised crime?
- What would be the impact of restricting overseas travel of registered child sex offenders on the rates of online offending worldwide?

*Research Innovative Technological Solutions to:*

- Detect live-streaming abuse
- Improve victim identification capacity
- Analyze CSEM in an automated manner (includes temporary analysis-time storage)? Can this be done legally by Industry?
- Better detect and prevent the proliferation of self-generated sexually explicit material on social media applications
- Protect children in their online activities from online child sex offenders (i.e. easy and affordable technological solutions for parents to install of their children's devices)
- Assist OCSE/transnational child sex offending investigations: how can technology (i.e. Artificial Intelligence) be utilized to defeat technological hurdles?
    - Improve mobile phone forensics
    - Identify and categorize known and unknown CSEM in seized electronic materials
    - Automatic detection of online child sexual ads (child prostitution)
    - Assess the effects of Industry involvement in the hosting and creation of services and tools for law enforcement on the open web and dark net

## Next steps

As the data collected in this e-scan confirms, OCSE and abuse offences are evolving and becoming more prevalent adding to the growing number of threats against children online. Technology will only become more advanced and the nature of the threat more substantial. Law enforcement, Industry and NGO members must collaborate further to combat this crime which has both devastating short term and long term impacts on children and youth worldwide. Looking ahead, the NetClean report (2018) cautioned law enforcement of even more advanced technological developments and emerging environments, such as virtual reality technologies, where CSE could soon manifest itself.

The findings from the e-scan as well as various consultations with other partners will inform the VGT strategic direction for the next three years.

## References


Altamura, A. (2017). Online Child Sexual Abuse and Exploitation: Spotlight on Female Offenders. *ECPAT International Journal, 12,* 26-42.

Canadian Centre for Child Protection (C3). (2016). *Child Sexual Abuse Images on the Internet: A Cybertip.ca Analysis*.

Canadian Centre for Child Protection (C3P). (2018). *National Strategy for the Protection of Children from Sexual Exploitation on the Internet.*

Canadian Police Centre for Missing and Exploited Children/Behavioural Sciences Branch (CPCMEC/BSB). (2015). *Global Alliance survey*. Ottawa. Canada.

*Criminal Code*, R.S.C., C-46 (1985).

ECPAT International. (2016). *Terminology guidelines for the protection of children from sexual exploitation and sexual abuse*. Luxembourg: Interagency Working Group on Sexual Exploitation of Children.

ECPAT International. (2017). *Online Child Sexual Exploitation: An Analysis of Emerging and Selected Issues*. Issue 12.

- The report contains four articles exploring some of the technical challenges and emerging concerns pertaining to the sexual exploitation of children online. Specially, it focuses on virtual currencies used by child sex offenders, the effectiveness of filtering and blocking access to CSEM, the role played by women in the commission of Internet-facilitated child sex offences, and the live streaming of child sexual abuse in the Philippines.

ECPAT International & INTERPOL. (2018). *Towards a Global Indicator on Identified Victims in Child Sexual Exploitation Material: Summary Report*.

- The study was financed by the European Union and carried out between 2016 and 2018 under the title International Child Sexual Exploitation (ICSE) Database Connectivity and Awareness Raising Enhancements (I-CARE) Project. It was based on quantitative and qualitative analysis and conducted in two parts:
    - Analysis of information for more than 1 million CSEM files in ICSE; and,

- Consultations with law enforcement personnel and experts in child sexual exploitation around the world.

European Parliament. (November 11, 2017). *Report on the implementation of Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography*. Retrieved from http://www.europarl.europa.eu/doceo/document/A-8-2017-0368_EN.html?redirect#title1

European Union Agency for Law Enforcement Cooperation (Europol). (2016). *On lawful criminal investigation that respects 21st century data protection*. Europol and ENISA Joint Statement. Retrieved from https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/on-lawful-criminal-investigation-that-respects-21st-century-data-protection.

European Union Agency for Law Enforcement Cooperation (Europol). (2017a). *Internet Organized Crime Threat Assessment (IOCTA)*.

- The report provides a law enforcement focussed assessment of the emerging threats and key developments in the field of cybercrime in 2017.

European Union Agency for Law Enforcement Cooperation (Europol). (2017b). *Serious and Organised Crime Threat Assessment (SOCTA)*.

- The report provides a detailed analysis of the threat of serious and organised crime facing the EU providing information for practitioners, decision-makers and the wider public.

European Union Agency for Law Enforcement Cooperation (Europol). (2017c). *Online Sexual Coercion and Extortion as a Form of Crime Affecting Children: Law Enforcement Perspective*.

- The report provides a law enforcement perspective the threat posed by online sexual coercion and extortion and recommends actions as part of the preventive campaign on this topic.

European Union Agency for Law Enforcement Cooperation (Europol). (2018). *Internet Organised Crime Threat Assessment (IOCTA)*.

- The report provides a law enforcement focussed assessment of the emerging threats and key developments in the field of cybercrime in 2018.

Global Alliance against Child Sexual Abuse Online. (2016). *2015 Threat Assessment Report*.

- Global Alliance member countries completed a questionnaire to assess the global threat of child pornography and related investigative challenges, and their answers were compiled in this threat assessment report.

INHOPE (International Association of Internet Hotlines). (2019). *INHOPE Statistics 2018*.

International Centre for Missing & Exploited Children (ICMEC), *Studies in Child Protection: Sexual Extortion and Nonconsensual Pornography,* 2018a. https://www.icmec.org/wp-content/uploads/2018/10/Sexual-Extortion_Nonconsensual-Pornography_final_10-26-18.pdf.

International Centre for Missing & Exploited Children (ICMEC), *Child Sexual Abuse Material: Model Legislation & Global Review*, 9th Edition, 2018b. https://www.icmec.org/wp-content/uploads/2018/12/CSAM-Model-Law-9th-Ed-FINAL-12-3-18.pdf.

Internet Watch Foundation. (2017). *Annual Report 2017*.

Internet Watch Foundation. (2018). *Once Upon a Year: Annual Report 2018*.

Krone, T. & Smith, R. (2017). Trajectories in online child sexual exploitation offending in Australia. *Trends & Issues in Crime and Criminal Justice, 524*.

- Exploratory study that examines data relating to a sample of offenders convicted of online child sexual exploitation offences under Australian Commonwealth law, to determine how online forms of child sexual exploitation and offline child sexual exploitation (contact offending), are related.

NetClean. (2018). A report about child sexual abuse crime.

- The data in this report has been collected through two different inquiries. First, data was collected from police officers across the globe who work on cases of child sexual abuse crime. The respondents, 272 police officers from 30 countries, contributed by filling out a survey anonymously through Griffeye's user portal. In-depth interviews with businesses and organisations from both the private and public sector that use NetClean ProActive to detect CSEM in their IT environments were also conducted.

New Zealand Police (2017). *Online Child Exploitation: Emerging Trends and the Pacific*. Intelligence Report.

- This assessment was prepared in close consultation with the Online Child Exploitation Across New Zealand (OCEANZ) and New Zealand Police workgroups including the High Tech Crime Unit, Pacific Island Chiefs of Police, Financial Intelligence Unit, Integrated Targeting and Operations Centre, and the Pacific Transnational Crime and Coordination Centre. Reports, international organisations, academic articles, law enforcement agencies, blogs and technology websites were also assessed.

NSPCC. (2016). *A Review of the Research on Children and Young People who Display Harmful Sexual Behaviour Online*.

Seto, M., Kingston, D., & Bourget, D. (2014). Assessment of the paraphilias. *Psychiatric Clinics of North America, 37(2),* 149-161.

*Sexting*. (2019). Accessed on January 19, 2019 from www.dictionary.com

UNICEF. (2016). *Victims are not Virtual.*

US Department of Justice. (2016). *The National Strategy for Child Exploitation Prevention and Interdiction*.

Virtual Global Taskforce. (2018). *Online Child Sexual Exploitation: Environmental Scan Survey*.

WeProtect Global Alliance. (2018). *Global Threat Assessment 2018*.

- At the Solutions Summit to End Violence against Children in Sweden on February 14, 2018, the WeProtect Global Alliance launched its Global Threat Assessment, the first ever research on the factors driving vulnerability to the threat of online child sexual exploitation and abuse at the global level.