Cybercrimes Convention
Online Child Sexual Exploitation and Abuse, Including CSAM

Definition
One of the most significant obstacles in the globally-connected fight against child sexual abuse and exploitation through ICTs is the lack of common terminology in general, and the lack of a universal definition for child sexual abuse material in particular. ECPAT uses the term Online Child Sexual Exploitation and Abuse (OCSEA), which it defines as situations involving digital, internet and communication technologies at some point during the continuum of abuse or exploitation. OCSEA can occur fully online or through a mix of online and in-person interactions between offenders and children.

Online Child Sexual Exploitation and Abuse (OCSEA) Child sexual exploitation and abuse online includes an evolving range of practices including: child sexual abuse material (CSAM), grooming children online for sexual purposes, live streaming of child sexual abuse and other related behaviors such as sexual extortion, the non-consensual sharing of self-generated sexual content involving children, and unwanted exposure to sexualized content.

Statistics
Prevalence data on OCSEA is limited, in part because it is a complex issue to measure. However, the results of extensive research conducted by ECPAT International, INTERPOL and UNICEF Innocenti across Southeast Asia and Southern and Eastern Africa reveals that between 1% and 20% of children had been subjected to OCSEA in the past year, although this is likely underreported.

In 2021, the National Center for Missing & Exploited Children (NCMEC) – the US-based global clearinghouse for Electronic Service Provider reports of child sexual exploitation - received 29.3 million reports containing 39.9 million images and 44.8 million videos. NCMEC further alerted law enforcement to over 4,260 potential new child victims[3].

If child sexual abuse material circulating online is being seen in increasing volumes, this is only the tip of the iceberg. Thanks to high-volume low-cost storage, the volume of CSAM found in the possession of offenders is ever increasing. For example, a June 2022 arrest in Australia recovered 10 terabytes worth of child abuse content; another in the USA recovered 58 terabytes of child abuse content.

INTERPOL maintains the International Child Sexual Exploitation Database (ICSE), a voluntary input victim identification tool for law enforcement that contains more than 2.7 million images and videos and has helped identify 23,564 victims worldwide[7]. ICSE facilitates essential police-to-police cooperation that is needed to identify the victims and offenders depicted in child sexual abuse material worldwide. Analysis of videos and images in INTERPOL's ICSE database conducted by INTERPOL and ECPAT International, published a joint report in February 2018, revealed that:
- The younger the victim, the more severe the abuse.
- 84% of images contained explicit sexual activity.
- More than 60% of unidentified victims were prepubescent, including infants and toddlers.
- 65% of unidentified victims were girls.
- Severe abuse images were likely to feature boys.
- 92% of visible offenders were male.

Long term impact
The impact of child sexual abuse and exploitation can be severe for victims and lifelong for survivors. In addition, recording the sexual abuse of a child in the form of images and videos is known to have a significant, lifelong impact on the victim. Nearly 70% of respondents to one survey have "indicated that they worry constantly about being recognized by someone who has seen images of their abuse"[1].

Beyond the physical, emotional and psychological impact on victims and survivors, the broader societal and economic costs of violence against children are estimated to be significant. There is limited data specific to sexual exploitation and abuse, and the paucity of prevalence data on violence against children more broadly makes it impossible to calculate the accurate cost by aggregating individual national estimates. However, robust national studies that have attempted an estimate have put the cost of violence against children at between US$3.7 trillion and US$7 trillion, or 4.5 - 8% of GDP in 2015[2]. In the case of child sexual exploitation and abuse, the low rates of disclosure and reporting mean that most of this crime type is hidden in terms of human, societal and economic impact.

Online child sexual exploitation and abuse crimes are almost invariably Inter-jurisdictional
The detection, investigation and prosecution of child sexual exploitation and abuse offences involving ICTs invariably requires inter-jurisdictional cooperation due to the cross-border nature of the Internet. An offender located in one place can produce and share images of child sexual abuse globally, or communicate with children for sexual purposes including for the production of child sexual abuse material in other countries. In addition, the electronic evidence of the crimes may be stored in jurisdictions other than that of the offender or victim.

ECPAT Sweden articulates that live streaming of sexual abuse cases in Sweden very clearly demonstrate inter-jurisdictional challenges in relation to:
> 1) Detection - cases are usually detected during other investigations;
> 2) Investigations – law enforcement need to travel to the country where the abuse took place to interview victims, obtain a green light to continue investigations in order to identify victims; and
> 3) Prosecution - the victims are underage, the guardian could be the abuser, and it is complex to work with different national systems without strong inter-jurisdictional laws and policies.

Case Study: CSAM Distribution for Financial Gain
The following case study was identified through the Disrupting Harm research conducted by ECPAT International, UNICEF Innocenti and INTERPOL.
In November 2017, a case was registered in northeast Thailand against a 30-year-old Thai male who was in possession of CSAM. It was alleged that he had abused 30 boys, aged between 12–13 years, for a period of one year to create and distribute material by posting images on his own Facebook page. All the children lived in the same vicinity as the offender and were living with their families. The victims were family members or neighbours of the offender. The Department of Special Investigation (DSI) received a tip from INTERPOL; the subsequent investigation revealed that the offender was earning money by selling CSAM using TrueMoney, Thailand's leading e-wallet for mobile networks. A New Zealand-based cloud storage and file hosting service was used to distribute the material, and its server was hosted in Europe. International cooperation was essential to investigate the case, conduct victim identification,

---

[1] Page 7, *Survivor's Survey – Executive Summary 2017*, Canadian Centre for Child Protection, available at: https://protectchildren.ca/pdfs/C3P_SurvivorsSurveyExecutiveSummary2017_en.pdf
[2] https://violenceagainstchildren.un.org/economic_costs_of_vac_viewpoint

and bring the offender to conviction. The offender was charged with online human trafficking and was sentenced to 146 years of imprisonment.

Hurdles and barriers to inter-jurisdictional investigations
- Lack of universal terminology and definitions of child sexual abuse material, leading to different definitions of and thresholds for crimes, and incompatible data sets between jurisdictions.
- Inconsistent laws and policies regarding online child sexual exploitation and abuse. Non- or incomplete ratification of international instruments to prevent sexual exploitation and abuse of children.
- Data privacy laws not permitting the sharing of data between law enforcement in different countries, which can aid investigations by enabling law enforcement to cross-check data, train and improve machine learning algorithms for forensic investigation and digital content triage.
- Insufficient expertise and capacity globally to investigate online child sexual exploitation and abuse crimes.

Recommendations to Ad Hoc Committee:
INCLUDE LANGUAGE PENALIZING CSAM FROM BEING PRODUCED AND CIRCULATING: The prevention of CSAM takes several forms, including prevention education and deterrence to stop the production of CSAM, and the use of technology to detect, report and remove CSAM from circulating online.

ALIGN TERMINOLOGY AND DEFINITIONS: Align terminology and definitions of CSAM, OCSEA, and electronic evidence with international guidelines. Ensure consistency in the definition of a 'child' as anyone under the age of 18 for all crimes of sexual exploitation.

ENABLE EXTRATERRITORIAL PROSECUTION: Include language for extraterritorial prosecution for all offences of sexual exploitation of children, including those occurring online. Do NOT require the principle of double criminality for proceeding with extraterritorial jurisdiction or extradition for sexual offences against children. Abolish statutory limitations for the prosecution of offences of all sexual exploitation of children.

ALIGN DATA CATEGORIZATION AND MANAGEMENT: Create the legal basis for aligning and/or adopting a common ontology for the labelling of child sexual abuse material.

ALLOW DATA SHARING: Provide the legal basis for law enforcement – to – law enforcement data sharing, namely of hash values of child sexual abuse material.

PROVIDE ADEQUATE RESOURCES: Increase and sustain resources for the investigation of online child sexual exploitation and abuse. Consider funding an international resource, such as Interpol, to assist in detection, investigation and prosecution of multi-jurisdictional child sexual exploitation and abuse.

ALLOW UNDERCOVER INVESTIGATION: Law enforcement often need to conduct undercover investigations to infiltrate online forums and communicate with CSAM offenders. Inconsistent legislation limits law enforcement's ability to generate and share evidence obtained through covert investigation.

REFER TO INTERNATIONAL INSTRUMENTS: Many international instruments exist in protecting children's rights including but not limited to Optional Protocols on the Rights of the Child, Protocol to Prevent, Suppress and Punish Trafficking in Persons (Palermo Protocol) which include crimes and definitions. If a member has ratified those instruments and the crime is committed via the internet, the crime should be punishable under the cybercrimes convention.

CONSIDER ROLE OF MULTISTAKEHOLDERS: Ending cybercrime will need the cooperation of the tech industry, law enforcement, judiciary and other stakeholders. These stakeholders should be able to legally demonstrate their commitment to the convention by ratifying same.