KINGDOM OF CAMBODIA

NATION RELIGION KING

Royal Goverment of Cambodia

# Initial situational analysis On Online Child Sexual Exploitation (OCSE) in Cambodia

2019

Cambodia National Council for Children

ក្រុមការងារបច្ចេកទេសអន្តរក្រសួង ដើម្បីពិនិត្យផ្តល់យោបល់ លើការសិក្សាស្រាវជ្រាវ
ការកេងប្រវ័ញ្ចផ្លូវភេទលើកុមារតាមប្រព័ន្ធអនឡាញនៅកម្ពុជា៖




ក្រសួងប្រៃសណីយ៍
និងទូរគមនាគមន៍
MINISTRY OF POSTS
AND TELECOMMUNICATIONS

សូមអរគុណដល់អង្គការដៃគូដែលបានគាំទ្រផ្នែកហិរញ្ញវត្ថុ និងបច្ចេកទេស៖

terre des hommes
stops child exploitation

APLE

Save the Children

PLAN INTERNATIONAL

ឧបត្ថម្ភដោយ៖

terre des hommes
stops child exploitation

# Contents

# Preface

Online Child Sexual Exploitation (OCSE) is a global issue that occurs in a variety of forms such as the production, possession and distribution of child sexual abuse material online with the intention of sexual exploitation or abuse, by using websites and social media platforms and smartphone apps to groom potential child victims online.

Although technology has improved the work and daily lives of many people in the world, it has also contributed to creating new challenges and new forms of crimes: kidnappings, illicit trafficking, abuse and sexual exploitation, especially against women and children, etc. These problems have grown and spread rapidly across the globe, especially in the region of Southeast Asia and the Pacific. Meanwhile, the use of popular electronic devices (smart phones, tablets, cameras ...), including by perpetrators of child sexual exploitation and abuse online, has turned into a new public concern. As a result parents, civil society, local authorities and children themselves need to work together to prevent OCSE and protect children in a timely manner.

The Royal Government of Cambodia, under the wise leadership of **Samdech Akka Moha Sena Padei Techo Hun Sen,** the Prime Minister of the Royal Government of Cambodia, has made significant progress in all sectors, especially in social and economic development. In the last two decades, Cambodia's economic growth had reached 7.7% on average and has allocated more budget to health, education, social services and other sectors to promote human development, including child development, to achieve the Sustainable Development Goals (SDGs) for 2016-2030 which focus on child welfare development. The Royal Government of Cambodia (RGC) is also paying attention to the implementation of international law, especially the Convention on the Rights of the Child, and additional protocols to address the needs of children such as protection for children to live in freedom, peace and development by formulating measures, including laws, policy, strategic planning and other regulations. The promotion and protection of children is a priority of the Royal Government of Cambodia and has been included in policies and programs, particularly the first strategy of the Fourth Rectangular Strategy: "**Human Resource Development"** and plans related to the protection and promotion of children's rights.

To protect the interests of children, Cambodia ratified the Convention on the Rights of the Child on October 15, 1992, and the Protocol to the Convention on the Rights of the Child. In addition, Article 31 of the Constitution of the Kingdom of Cambodia recognizes and respects human rights as stipulated in the United Nations Charter, the Universal Declaration of Human Rights and the Covenant, and conventions related to human rights, women's and children's rights. Article 48: The State guarantees the protection of the rights of children enshrined in the Convention on the Rights of the Child, especially the right to life, the right to education, the right to be protected in the event of war, and the protection against commercial or sexual exploitation of children. The State protects against involvement in the workforce that could jeopardize a child's education or that endangers his health or well-being.

Cambodia has been more and more integrated into the region and the world, which opened many opportunities to build and develop the country. At the same time, the Royal Government of the National Assembly of the 6th mandate has set its Fourth Rectangular Strategy, National Strategic Development Plan (NSDP) 2019-2023, The Sustainable Development Goals (SDGs) 2016-2030 have prepared the ground for the 4th Industrial Revolution, with a particular focus on technology, to reinforce the functionality and efficiency of political systems and economic and

social services the progress of global Information Technology (IT) has spread to all countries, including Cambodia. Information technology has contributed to Cambodia's growing political, economic and social services and communication at the regional and global level.

Seeing the implications and challenges that have recently emerged, the Royal Government of Cambodia has joined the Global Partnership for the Elimination of Violence Against Children (Pathfinding Country) on September 12, 2019. At that time, the Royal Government of Cambodia also signed the (WePROTECT) Declaration in Abu Dhabi in 2015 on Prevention of Online Child Sexual Exploitation (OCSE), with the Ministry of Interior as the mediator. This positive progress is linked to the Action Plan to Prevent and Respond to Violence Against Children 2017-2021, which also included actions to prevent Online Child Sexual Exploitation (OCSE).

To address the above challenges, the General Secretariat of the Cambodia National Council for Children (CNCCGS) cooperates with partner organizations to conduct an analysis of the situation and impact of Online Child Sexual Exploitation (OCSE) in Cambodia. The research questions included the following: where and how children are at risk, as well as the current state of capacities and gaps in national policy, legislation, criminal justice, social services, and the private sector in order to identify actionable, evidence-based recommendations for Cambodia-specific interventions, based on the WePROTECT Model National Response (MNR), and to draw lessons from local and international best practices.

I'd like to thank the OCSE Technical Working Group from the Ministry of the Interior, the Ministry of Defense, the Ministry of Posts and Telecommunications, the Ministry of Education, Youth and Sport, the Ministry of Social Affairs, Veterans and Youth Rehabilitation, The General Secretariat of CNCC and Terre des Hommes Netherlands in Cambodia, Action for Children (APLE), Save the Children and related organizations that provided technical and financial support to this situational analysis to assess the current threat of Online Child Sexual Exploitation (OCSE) in Cambodia.

Phnom Penh, January 10, 2020
President of CNCC

**Vong Sauth**

# Acknowledgements

OCSE is an emerging form of child sexual abuse and exploitation that is mediated by the internet, utilising websites and social media platforms and smartphone apps. The Royal Government of Cambodia is a signatory to the WePROTECT Statement of Action signed at the Global Summit in Abu Dhabi in 2015. The WeProtect Model National Response (MNR) stresses the importance of engagement of different stakeholders and identifies industry as key stakeholder to protect children online.

This situational analysis assesses the current threat of Online Child Sexual Exploitation (OCSE) in Cambodia, estimates that the social media and use of technology has expanded dramatically in recent years. And this trend is predicted to continue in the future in Cambodia. This OCSE situational analysis aims to identify actionable, evidence-based recommendations for Cambodia-specific interventions, based on the WePROTECT Model National Response (MNR), drawing on learnings from local and international best practice.ECT, which will be integrated into the Action Plan for Responding to OCSE in Cambodia.

I would like to express my deepest gratitude to **Samdech Akka Moha Sena Padei Techo Hun Sen**, the Prime Minister of the Royal Government of Cambodia and Honorary President of the Cambodia National Council for Children and **Samdech Kittipritbandit Bun Rany Hun Sen**, wisely led the rehabilitation and development. The nation is prosperous in all respects, including its connection to the interests of children and to give mercy to all children.

I would like to express my appreciation and appreciation to the Cambodia National Council for Children, the National Child Protection Committee, the OCSE Technical Working Group, the relevant ministries, Terre des Hommes Netherlands in Cambodia, Action for Children (APLE), Save the Children and related organizations that provided technical and financial support to this situational analysis to assess the current threat of Online Child Sexual Exploitation (OCSE) in Cambodia. I sincerely hope that after the "evidence-based recommendations" are identified, we will continue to actively participate in action plan development to respond to, prevent and intervene in the interests of Cambodian children.

Phnom Penh, ……., 2020

Secretary General of CNCC

# Definitions & Acronyms

This situational analysis uses the following definitions, largely derived from the Luxembourg Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse (2016) and WePROTECT Global Alliance (2016).

**OCSE** Online Child Sexual Exploitation. This is an emerging form of exploitation and child sexual abuse that is mediated by the internet, which includes the production, possession and distribution of online CSAM, live-streaming of CSEA and the grooming of potential victims.[1]

**CSEA** Child Sexual Exploitation and Abuse. This is an inclusive term for both sexual abuse and exploitation by an adult. Sexual exploitation involves sexual contact with the child in exchange for some form of remuneration, which can be monetary, but children may only receive food or somewhere to sleep. Sexual abuse is understood as sexual contact with the child's private areas with or without their consent and with or without physical force. Abuse requires no element of exchange, and can occur solely for the sexual gratification of the person committing the act.[2]

**CSAM** Child Sexual Abuse Material. Otherwise known as 'child pornography', this term refers to any material depicting acts of sexual abuse and/or focusing on the genitalia of the child.

**CSEM** Child Sexual Exploitation Material. This term is generally used in a broader sense to encompass all sexualised material depicting children, including 'child sexual abuse material'.[3]

**UNODC** United Nations Office on Drugs and Crime. This is the UN agency tasked to fight against illicit drugs and international crime. In recent years, this agency, along with Interpol, has become greatly involved in the law enforcement aspects of responses to OCSE.

**NCMEC** National Center for Missing and Exploited Children. Based in the United States, NCMEC is a private, non-profit organization that provides information to help locate children reported missing and to assist physically and sexually abused children. The organization has become an integral part of global reporting and referrals for child sexual abuse materials.

**Live Online Child Sexual Abuse** This refers to live transmission or broadcast of child sexual abuse to viewers through "streaming" over the internet, which allows viewers to watch and engage instantaneously, while the abuse is occuring.[4]

[1] Interagency Working Group on Sexual Exploitation of Children (2016), "Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse". Retrieved from: http://luxembourgguidelines.org/.
[2] *Ibid.*
[3] *Ibid*.
[4] *Ibid.*

**Grooming** Within the context of child sexual abuse and exploitation, this refers to the solicitation of children for sexual purposes. Online grooming, within the context of OCSE, refers to the process of establishing/building a relationship with a child either in person or through the Internet or other digital technologies to facilitate either online or offline sexual contact with that person.[5]

**Sextortion** Sexual extortion. This refers to 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 her/him under the threat of sharing the material beyond the consent of the depicted person (e.g. posting images on social media).[6]

**Sexting** Sending self-produced sexual images of sexual images, or "the exchange of sexual messages or images" and "creating, sharing, and forwarding of sexually suggestive, nude, or nearly nude images through mobile phones and/or the Internet".[7]

**MNR** Model National Response. Rising from the 2015 WePROTECT summit in Abu Dhabi, this model provides guidance and support to countries and organizations to helping to build a response to OCSE encompassing a wider set of capabilities to prevent to ensure a complete national response to the issue.

**ECPAT** A global network of civil society organisations, based in Bangkok, that works to end the sexual exploitation of children. The name is an acronym for "End Child Prostitution and Trafficking".

**ISP** Internet Service Provider. This is an organization that provides services for accessing, using, or participating in the Internet.

**ICT** Information and communications technology (or technologies). This is a broad and generally-accepted term referring to all devices, networking components, applications, and infrastructure allowing modern-day computing and internet use.

**HCD** Human-centered design is a creative approach to problem solving, which starts with listening to, and learning from, people and ends with new solutions that are tailor-made to suit their expressed needs. Human-centered design builds upon participatory action research, moving beyond solely documenting participants responses, working with them to produce unique solutions to complex problems.

[5] *Ibid.*
[6] *Ibid., 52*
[7] *Ibid., 44*

# Executive Summary

This situational analysis assesses the current threat of Online Child Sexual Exploitation (OCSE) in Cambodia, its various forms within Cambodian communities, where and how children are at risk, as well as the various capacities and gaps in national policy, legislation, criminal justice, social services, and the private sector in order to identify actionable, evidence-based recommendations for Cambodia-specific interventions, based on the WePROTECT Model National Response (MNR), drawing on learnings from local and international best practice.

OCSE is an emerging form of child sexual abuse and exploitation that is mediated by the internet, utilising websites and social media platforms and smartphone apps. It includes the production, possession and distribution of child sexual abuse material online, the grooming of potential child victims online with the intention of sexual exploitation or abuse, and Live Online Child Sexual Abuse[8].

Globally, access to affordable internet, personal computers and smartphones is rapidly increasing throughout vulnerable communities in Cambodia and mobile internet connectivity, social media and use of technology has expanded dramatically in Cambodia in recent years. Presently, nearly half of Cambodians haves at least one smartphone (a 21% increase from 2015) and another 48% cite using Facebook[9]. While internet and internet-capable devices are becoming more available, they are also becoming more affordable, with personal computers, and smartphones readily available and accessible in low-income communities which potentially poses significant risks for children and young people who tend to be advanced users of the Internet and actively participate in social media.

At present, little is known in Cambodia about the existence and magnitude of OCSE (APLE, 2016) and community awareness is minimal[10]. The Cambodian Action Plan to Prevent and Respond to Violence Against Children (2017-2021) identifies clear gaps in legislation, the capacity of law enforcement, community awareness, and private industry response to the issue on OCSE. The Royal Government of Cambodia is a signatory to the WePROTECT Statement of Action signed at the Global Summit in Abu Dhabi in 2015. The WeProtect Model National Response (MNR) stresses the importance of engagement of different stakeholders and identifies industry as key stakeholder to protect children online.

**Methods**: This situational analysis utilizes learning workshops, online surveys, and in-depth discussions to develop a comprehensive understanding of the nature and extent of OCSE in Cambodia at the community level, including an assessment of the various child-protective capacities government, criminal justice, civil society, and private industry. The study aims to identify actionable and evidence-based recommendations for Cambodia-specific interventions, based on the WePROTECT Model National Response (MNR) framework, which will feed into the development of an action plan to address OCSE in Cambodia.

Learning workshops inform the core inquiry of this study and explore the various forms of OCSE that experienced among children in Cambodia. Thirteen learning workshops were conducted with 220 children aged 8-17 and 45 teachers from public schools, private schools, and NGO school centers in three areas of Cambodia: Sihanoukville, Siem Reap, and Phnom Penh. In addition, three workshops were conducted with 45 school teachers throughout the three areas in order to develop an understanding of how teachers think about and interact with child protection issues in an online environment. With regard to the assessment of child-protective capacities, a total of 45 in-depth interviews were conducted with key representatives from national, regional, and international law enforcement, government agencies, and child-protection organizations, as well as relevant members of the Cambodian private sector. The interviews assess general awareness of OCSE and respondents' various capacities to respond

[8] WePROTECT. (2016).
[9] UNICEF. (2016).
[10] Ministry of Women's Affairs. (2014).

to the needs of children and collaborate with relevant partners and agencies prevent abuse and exploitation of children on the internet in Cambodia.

Lastly, an online survey was conducted with 139 public school youth in Battambang province. While the initial intention of the research was to collect a nationally-representative sampling of Cambodian youth in public, private, and vocational training schools, due to time and political constraints, the breadth of survey was limited. The data represented in these surveys are in no way representative of the nation as a whole, however, it offers a useful set of learnings about internet use among this particular group of youth and provides potentially important comparison to the other learnings developed throughout this study. The findings of this survey are included as an annex in this report and are reflected upon within the study's main discussion and recommendations. It is our intention that future research initiatives will work with the Royal Government of Cambodia, through the Cambodia National Council for Children (CNCC) to build upon these limited findings and develop a nationally-representative sample of Cambodian youth in public, private, and vocational training programs.

Children and Community: Children demonstrate a clear picture of the nature of OCSE related risk at the community-level and indicate a significant awareness of OCSE-related risk in their online environments. Out of 47 'working groups' of children across the 13 learning workshops with children, 28% describe an awareness of how various internet platforms (especially Facebook) is used as a platform for grooming of children for sexual exploitation in both online and offline environments, 27% describe the solicitation and distribution of child Sexual abuse Materials (CSAM) as a high risk, 24.1% describe various forms of live-streaming sexual exploitation, and 60.3% of working groups describe the distribution of adult pornographic materials and CSAM from adults to children as a high risk in their online environments.

Out of 220 child-participants in learning workshops throughout the three metro areas, 37 children or 17% (about one-in-six) share at least one personal experience of OCSE-related risk on the internet. The majority, or 29 of these 37 children describe OCSE in the form of grooming or various forms of sexual advances by adults online. Overall, one-in-four children (25%) share various personal (18) or second-hand (11) accounts of grooming or sexual advances by adults online, one-in-five (20%) share a diverse range of scenarios in which adults, other children, and online advertising exposes them to various kinds of explicit pornographic materials online, and six children (5%) share instances of having sexual images of themselves or other children taken and/or circulated on the internet.

In addition to these findings, 2018 reporting (from January to November) to US Homeland Security Investigations (HSI) in Phnom Penh from the National Center for Missing and Exploited Children (NCMEC) shows a 490% increase of Cambodian CSAM reporting (from 25,332 in 2017 to 123,896 in the first 11 months of 2018). More significantly, nearly a third of these reports (29% or 35,913) are considered to be new and actionable, potentially signaling an increase not only in the circulation of CSAM in Cambodia, but also the production of new materials.

**National child-protective capacities:** Seniors leadership of the Anti-Human Trafficking and Juvenile Protection Department (tasked with responding to various forms of sexual exploitation and violence against children) do not indicate a strong awareness of OCSE in general or the breadth of the internet's role as a venue for child sexual exploitation within Cambodian communities. The majority of awareness seems to center around traditional cases of child sexual abuse and exploitation, in which a perpetrator uses an online platform (especially Facebook) to arrange to meet a child for offline abuse and overlook or discount exploitation that happens in a purely online environment. Even so, though the understanding on OCSE or to aware the way and scope of internet which is easy way to child abuse and exploitation in communities is limited.

Further, the Cybercrime Unit, which is the de-facto unit to carry the responsibility of providing follow up and investigation for OCSE-related crimes, is a small team which does not yet have the capacity to investigate crimes committed on the internet. Rather, the unit's specialization

focuses on the physical, forensic investigation of evidence held on electronic devices gathered from criminal raids. This overlooks the majority of OCSE-related crime and indicates a significant gap in the nation's ability to effectively address the issue of OCSE.

**Overall barriers within national criminal justice** were found to include a lack of modern technologies and knowledge on information and communication technology (ICT) used by youth and the key trends of technology, a lack of resources to investigate at community level, a lack of connection with technical expertise and existing international resources, and an overreliance on traditional, physical methods of investigation, which are not greatly helpful for crimes committed in a digital context.

**Key recommendations:** Children and their teachers emphasize the need for online safety training and issue-level awareness raising around OCSE, including training on 1). how to better use privacy settings on social media to keep their pictures and personal information safe, 2). how to set a stronger password to protect users' accounts, and how to understand and 3). avoid the practices of online predators. In addition, teachers and students indicate the need for parents to be more aware of their children's online environments and more greatly engaged with their children's online lives. While teachers cite this as a need for child safety, children in learning workshops also seem to welcome the idea of positive parental engagement into their digital worlds.

The research recommends the development of a "multi-stakeholder unit", interdisciplinary, and cross-sectoral national body of all entities that hold a responsibility to protect children in an online environment, including civil society and private industry. Such an effort should, ideally, be government-led and situated at the senior leadership of government official staff and law enforcement. In addition to the development of a practical body, the research provides a set of recommendations child-protection capacities within Cambodia including the development and specialization of the CyberCrime Unit to allow for proactive collaboration with police, civil society, US Homeland Security, and other relevant partners to respond crime cases, process cases, build intelligence, and conduct specific investigations— especially with regard to existing cases referred by NCMEC to US Homeland security.

Within this context, the research identifies an immediate need to establish a secure connection between Phnom Penh NCB office and Interpol, which would aid in unifying the process of dealing with CSAM to ensure that all images are hashed, indexed, and access is given to international law enforcement. In addition, efforts should be made to bring Cambodian law enforcement up to a sufficient standard to allow for the establishment of an official connection with Interpol's International Child Sexual Exploitation (ICSE) Database, which would enhance the operational capability of Cambodian law enforcement in the process of identifying victims and offenders throughout the nation and provide a wealth of international tools and resources with which to better address the issue of OCSE throughout the nation.

# Chapter 1: Introduction (Literature)

Online Child Sexual Exploitation (OCSE) is an emerging form of exploitation and child sexual abuse that is mediated by the internet, utilising websites and social media platforms and smartphone apps. It includes the production, possession and distribution of child sexual abuse material online, and the grooming of potential child victims online with the intention of sexual exploitation or abuse, including live streaming of child sexual exploitation and abuse[11]. Globally, access to affordable internet, personal computers and smartphones is rapidly increasing within poor and vulnerable communities. Within Southeast Asia, 75% of people have a mobile phone and more than two thirds of internet users access the web through mobile devices[12]. There are at least 750 million social media users across the region[13].

Mobile internet connectivity, social media and use of technology has expanded dramatically in Cambodia in recent years; that trend is predicted to continue. At present, there are 19.5 million mobile phones registered in Cambodia, or 119% of the country's total population[14]. Data collected in 2016, by interviewing 2,061 participants aged between 15 and 65 year olds across Cambodia, shows that 48% of Cambodians were found to have at least one smartphone, a 34% increase from 2015. It also shows that Facebook use among Cambodians continues to grow. Based on this data, 48% of Cambodians say they use or have used Facebook (an increase of 34% from 2015, 23% from 2014 and 16% from 2013). The figure is significantly increased compared to 2015 is 39%, similar to 106% increased in 2014 and 200% in 2013. Men reported using Facebook more than women (55% versus 41%)[15]. In 2019, Men used Facebook increased more than women (59% versus 41%)[16]. Little is understood in Cambodia about the specific online threats for children; however, OCSE is of increasing concern as global sources indicate that advances in internet and mobile technology contribute heavily to sexual exploitation of children in travel and tourism.

Access to affordable internet, personal computers, and smartphones in low-income communities has many social and economic advantages. However, it also poses significant risks for children and young people who tend to be advanced users of the Internet and actively participate in social media. This expansion of the internet has made child sexual abuse material more accessible, and has allowed for easier and faster dissemination of pro-pedophile literature among paedophiles and those with sexual interests in children[17]. As internet subscription fees lower and connection speeds increase, larger data transfers can be sent between users. The expansion of internet use has also allowed for the creation of supportive communities for perpetrators across regional and international boundaries[18], thereby giving a pseudo sense of legitimacy to people with sexual interest in children[19]. While the number of victims of OCSE globally is not known, the number of websites containing child sexual abuse material is cited to have increased by 147% between the years of 2012 and 2014 alone and recent estimates suggest that it is a significant problem which is rapidly increasing[20].

[11] WePROTECT. (2016).
[12] We are Social. (2017).
[13] *Ibid*.
[14] TRC-2018
[15] Open Institute-2016
[16] Geeks in Cambodia-2019.
[17] Elliott & Ashfield. (2011); Kierkegaard. (2008).
[18] US Department of Justice. (2018); INTERPOL. (2018).
[19] Kloss, et al. (2014).
[20] UNICEF. (2016).

# 1.1. Forms of OCSE

## 1.1.1 Child Sexual Abuse Material (CSAM) Online

The majority of regional literature available on OCSE tends to focus on the production and distribution of child sexual abuse materials (CSAM), otherwise known as 'Child Pornography'. A number of international organizations, such as INHOPE, Internet Watch Foundation, and National Center for Missing and Exploited Children (NCMEC) work collaboratively with interpol, national law enforcement agencies, and internet service providers to remove CSAM and prosecute offenders[21]. Online CSAM often requires a collaborative response in order to remove materials and prosecute offenders in that the phenomenon is, by nature, a transnational issue. Children may be abused in one country, but their images are distributed and hosted on and through servers located in other countries—thus this issue often involves multiple crimes taking place in and through multiple countries. This is further complicated when the producer and/or distributor of CSAM in a host country is a foreign national.

Online offender communities remain a key concern in this area of OCSE. Such communities operate from the Darkweb, which provides a safer and anonymous environment for offenders to share CSAM with other offenders and to form social networks of like minded people, which creates a false sense of legitimacy for their behaviour[22]. Further, a great deal of CSAM is produced for the purposes of distribution, as opposed to solely for the personal use of the abuser. Some European nations have reported a growing trend of the production of CSAM on demand as a means of income generation for the producer, however these businesses are still not fully understood[23].

## 1.1.2 Live-streaming

Live-streaming Online Child Sexual Exploitation is an emerging form of online child sexual exploitation (OCSE), which involves viewing or direct live-streaming video footage of children performing sexual acts in front of a webcam or cellphone camera for an adult(s) in exchange for remuneration to the child, a parent, or a broker[24]. With the exception of the Philippines, there has been little discussion on the vulnerabilities of children in the ASEAN region with regard to the use of live-streaming services for the sexual abuse and exploitation of children. Much of the response to OCSE within government and CSO sectors has focused on identifying CSAM and related materials, but has overlooked the rapid growth of live streaming apps such as Bigo Live, CubeTV, Magic Video, Blued, LiveChat, App Live, among others. Most of these apps purportedly exist as social media platforms through which users are able to live-stream parts of their daily life. However, many of the apps are increasingly used as a means for contacting victims and sharing exploitative materials[25]. Once contact has been made, users have the option of going into a private chat or using other social media services, many of which provide end-to-end encryption, where exploitation and abuse can occur and at times be recorded.

## 1.1.3 Sexual Grooming

As the area of online child sexual exploitation is relatively new, most of the available literature explores the process of grooming for abuse within the physical, offline world, and does not explore the specific dynamics of grooming online[26]. Presently, children have been known to

[21] NetClean. (2017).
[22] Europol. (2017).
[23] *Ibid.*
[24] Terre des Hommes-Netherlands. (2018).
[25] Europol. (2017).
[26] Kloss et al. (2014).

become involved individually, through online grooming or by taking part in a larger family-run or neighborhood 'business'.

Sexual grooming is understood as the process by which an offender prepares a child for sexual abuse[27], and involves the organisation and utilisation of various opportunities aimed at gaining the trust of a child[28]. This process may be subtle and often involves recurring acts, characterised by the building of trusting relationships and eventual abuse of trust with the child[29]. It is important to acknowledge that in many settings the grooming process is not limited to the child or children, but also parents, caregivers, extended family and others in a position of trust—and who may present a barrier to the potential perpetrator or facilitate the process.

### 1.1.4 Self-Generated Sexual Images

Sending sexual images (or 'sexting') is a growing trend among children and young adults. In many contexts this may seem harmless, however, an analysis from INHOPE Foundation notes a rise in digital crimes such as coercion and extortion, which are increasingly the result of self-generated sexual images[30]. This is a trend that should not be understated as images such as these can be used to control and exploit youth into providing ransom or even further explicit images in exchange for the protection of the youth's privacy.

### 1.1.5 Online and Offline CSEA

The definition of online and offline CSEA is often blurred, particularly with the rapid evolution of internet platforms and devices. Because of this, CSEA with some online component is increasingly common. The International Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse also acknowledges this blurred line and cites that, rather than seeing online exploitation as a distinct type of sexual exploitation, in and of itself, it is important that the Internet is seen as, more broadly, as a potential means to exploit children sexually[31].

One of these areas that may commonly go overlooked is the growing use of phone 'hook up' apps such as Grindr, Badoo, OkCupid, Jack'd, etc) and other platforms, which are easily accessed by children and youth. While platforms such as these have policies against user accounts for people under the age of 18, children can easily create accounts by stating that they are over the age of 18. On these platforms, children can virtually meet adults in the app, where sexual grooming and the exchange of sexually-explicit images can occur, and then later in-person meetups can be arranged, where further abuse can take place.

Europol has identified sexual coercion and extortion (SCE) of children as a key concern within this context. Offenders commonly initiate contact with children using fake profiles representing themselves as other minors and will often be in contact with multiple children simultaneously—often maintaining multiple profiles across multiple social media platforms, allowing them to target different children with different fake personas[32].

## 1.2 The Response

In response to CSAM in Cambodian, a number of local and international organizations are working to make children safer on the internet by responding to the threat of OCSE. This includes global monitoring and tipline organizations, which work to identify and remove online

[27] Craven, et al. (2006).
[28] McAlinden. (2006).
[29] Finkelhor, D., & Wolak, J. (2004).
[30] INHOPE. (2016).
[31] Terre des Hommes. (2018); ECPAT International. (2016).
[32] Europol. (2017).

CSEA, offer a reporting platform, analyse content, and route CSAM cases to the necessary local governments for investigation and prosecution. Some key organizations working to respond to OCSE include:

- **Ministry of Interria (MoI):** There are a specialist unit have been working and carrying out the tasks of prevention OCSE, as well as working on the mechanism and formulating a standard policy to respond and to address the issues.
- **Ministry of Post and TeleCom (MoPTC):** A professional body has been working and carrying out the tasks of supporting the protection of children against OCSE through the telecommunication regulator, establishing technical policy, regulatory and internal standards.
- **MoSAVY:** Cambodia National Council for Children (CNCC), Is mandate for inter-ministry coordination enables them to play a unique coordinating role for mainstreaming OCSE activities into national-level policy development and the multi-sectoral implementation of a NAP on OCSE.
- **Terre Des Hommes-Netherlands (TdH-NL)** has pioneered innovative approaches to addressing OCSE with the 'Sweetie', research and global campaign, and in many respects is considered to be a world leader in this area.
- **Action Pour Les Enfants (APLE)** has contributed significantly to the prevention and protection of children across the social spectrum, for over a decade and have lead on national initiatives to address online abuse and exploitation, including setting up of a national Internet Hotline in collaboration with the InHope Foundation. They are well connected and respected within government and able to take their messages and to the highest levels of government.
- **International Association of Internet Hotlines (INHOPE)**[33] is an umbrella organization based in Netherlands which collaborative a global network of 45 hotlines in 40 countries. INHOPE receives reports of suspected online CSAM including child sexual abuse material from the members around the world. The Hotline will investigate and pass to relevant law enforcement agency and ISP hosting the content, if found illegal.
- **The National Center for Missing and Exploited Children (NCMEC)**[34], which is a US-based NGO, funded by the United States Department of Justice since 1984. NCMEC provides data and analytics on the production and distribution of CSAM through its Cyber Tipline, and as the resource for missing and exploited children as a focal point in providing assistance to raising public awareness about child abduction, molestation, and sexual exploitation and recovering missing children. NCMEC along with the Center for Missing and Exploited Children (CMEC) and the International Center for Missing & Exploited Children (ICMEC) runs a global missing children's network of 22 countries and train law enforcement personnel, work with law enforcement and legislatures to adopt new laws combating child pornography in over 100 countries.
- **Internet Watch Foundation (IWF)**[35] is a UK-based NGO set up in 1996 that provide an internet Hotline for the public to report potentially criminal online content to be notice and takedown. IWF is recognized as agency for reporting, handling and combating child sexual abuse images on the internet. IWF has core work to remove of online child sexual abuse images and videos with IWF's remit to inform the host or ISP to quickly remove or disable access to the potentially criminal content. IWF is a founder member of INHOPE and association of Hotlines to contribute on the protection of children on the internet and

[33] INHOPE Foundation. *At A Glance.* Accessed 20 Nov 2018 from, http://www.inhope.org/gns/who-we-are/at-a-glance.aspx
[34] NSVRC. Accessed 20 Nov, 2018 from, https://www.nsvrc.org/organizations/60
[35] Internet World Foundation. *Who We Are.* Accessed 20 Nov, 2018 from, https://www.iwf.org.uk/what-we-do/who-we-are

work in partnership with the police and the host company to remove the content and investigate its publishers.

- **Cybertip.ca**[36] is a Canada-Based NGO since 2002. Cybertip.ca's goal is to reduce child victimization by providing national programs and services to the public. Cybertip.ca operates as a front door to the public for reporting about information or content related to possible online child sexual exploitation and the Cybertip.ca web server receives the information in a secure fashion and prioritized for processing, classification based on the Criminal Code (Canada) for analyst. The report is sent to the appropriate law enforcement agency and/or INHOPE partner hotline and appropriate agencies, if the information potentially illegal incident.

# 1.3 The Cambodian Context

At present, little is known in Cambodia about the existence and magnitude of OCSE[37] and community awareness is minimal.[38] The Cambodian Action Plan to Prevent and Respond to Violence Against Children (2017-2021) identifies clear gaps in legislation, the capacity of law enforcement, community awareness, and private industry response to the issue on OCSE. Within this context, there is growing concern among stakeholders working in child protection in Cambodia that there is an imminent need to design counter-mechanisms to address this issue— a task which is challenging and one which will require a joint multi-sectoral commitment.[39] While official figures on OCSE do not exist, the National Plan of Action to Prevent Violence Against Women (2014-2018) cites an increased identification of the production, possession and distribution of CSAM online, the grooming of potential child victims online and live streaming of child sexual exploitation and abuse (CSEA)[40].

The Royal Government of Cambodia is a signatory to the WePROTECT Statement of Action signed at the Global Summit in Abu Dhabi in 2015. The WeProtect Model National Response (MNR) stresses the importance of engagement of different stakeholders and identifies industry as key stakeholder to protect children online. In particular, the Cambodian Action Plan on Violence Against Children recommends specific amendments to the draft cybercrime law ensuring full protection from OCSE including sexual extortion, sexting, live streaming, and online grooming. It also calls for local law enforcement to be given the authority to investigate, confiscate equipment, and block content "of any online platform contributing to, promoting or facilitating" OCSE. Further, it recommends amendments to the existing telecoms law to include child protection protocols for online and mobile platforms[41].

## 1.3.1 Policy-level protections

There are currently significant gaps in legislation surrounding OCSE in Cambodia. In 2008, the Royal Government of Cambodia enacted the Law on Suppression of Human Trafficking and Sexual Exploitation. While the law criminalizes 'child pornography', it does not criminalize does not have explicit provisions that criminalize accessing or downloading child pornography images, or the possession of CSAM without the intent to distribute. Further, distribution and dissemination is criminalized in 'public spaces', which ignores CSAM traded or distributed within non-public areas. There are also no provisions for accessing or downloading CSAM for sexual grooming. In addition, there is no provision which requires ISPs to report CSAM to law

[36] Cybertip.ca. *About us.* Accessed 17 Nov, 2018 from, https://www.cybertip.ca/app/en/about
[37] Action Pour Les Enfants. (2016).
[38] Ministry of Women's Affairs. (2014).
[39] Action Pour Les Enfants.(2016).
[40] Ministry of Women's Affairs. (2014).
[41] UNICEF. (2017).

enforcement or other authorities[42]. Some of these gaps were intended to be filled with the anti-cybercrime law, however this law has been in draft form since 2012 and still has yet to be ratified.

## 1.3.2 Mobile Phone and Internet Use and Access in Cambodia

A 2018 survey by LIRNEasia, pro-market Asia Pacific think tank, finds 91% of Cambodian households have at least one mobile phone and rural-dwellers 21% less likely to own a mobile compared to those in an urban setting[43]. Smartphone penetration is high among urban residents, compared to rural (60% vs. 44%) and is most common among Cambodian young people: 78% among those aged 20-24, 70% among those aged 15-25, and 59% among those aged 15-19. Among those who cite not using an internet-connected phone, main barriers to use is affordability (50%), lack of digital skills and literacy (41%), and feeling that it is too complicated to use (30%)[44]

According to TRC data, In 2018 report there are 36 companies provide internet service in Cambodia. Among Telecom company that provides internet service to the clients is Smart (42%), Metfone (40%), Cellcard (14%), and other companies (4%). At that time, permanent internet service companies used is Metfone (49%), Smart (12%), Shimeng (10%), Kogitel (8%), Shinvei (7%), Tel-cotech (5%) and others (9%). [45]There are more than 30 companies provide internet service in Cambodia, according to a 2014 report by the United Nations Development Program (UNDP). Further, 4G networks in Cambodia have low (good) latency compared to other Southeast Asian nations[46]. The most commonly used telecom company in Cambodia is Metfone, used by 45% of the sampled population, followed by Smart (40%), and Cellcard (14%). More than two in three youth, or 68%, use Metfone, followed by Smart (41%). Rural dwellers are more likely to use Metfone while urban dwellers are more likely to use Smart. According to LIRNEasia, mobile internet (3G, 4G, LTE) users in Cambodia spend about $2.6 and half of young people spend $2 or less a month on internet service.

According to UNDP, Cambodians most commonly use mobile phones for making and receiving calls (98%), listening to the radio (43%), sending and receiving messages (32%), playing/downloading games (27%), and taking photos (22%)[47]. Cambodian social media users were found to be less willing to share personal information, such as their gender, real name, age, marital status, mobile number, email address, religion, political views, sexual orientation, pictures, or video of family and friends[48]. More than one-in-four Cambodian internet users, or 26%, have experienced online harassment, with higher disclosure of harassment among females users in comparison with males (29% vs. 23%). Two-thirds of internet users, or 65%, cite worrying about their privacy information, 63% believe that people can become addicted to mobile phones and the internet, 47% cite concerns about children's exposure to inappropriate content, and 24% cite that the internet affects social division, and 20% cite turning down spending time with their family or friends in order to spend time on social media.

## 1.3.3 National Reporting Mechanisms

**Cambodia National Police Commissioners (Hotline 117)**- This hotline is publicly for report and respond to all issues and crime. Meanwhile, have one more hotline is 1288 for special report and respond to anti-trafficking and judicial justice. Also, Cambodia National Police

[42] World Bank. (2015).
[43] LIRNEasia. (2018).
[44] *Ibid.*, 22.
[45] TRC: 2018
[46] Benchmarks from IMDA Singapore 300 ms for an International server, 100 ms on 4G / LTE
[47] UNDP. (2014).
[48] LIRNEasia. (2018).

Commissioners in collaboration with local and international NGO working on OCSE on prevention, protection and respond towards OCSE.

**Internet Hotline Cambodia (IHC)**[49] — In 2015, the APLE Internet Hotline was established with the support of INHOPE Foundation and run by APLE Cambodia which offer public to anonymously report on CSAM. In coordination with the Anti Cybercrime Department of MoI and other INHOPE hotlines and internet industries to takedown contents and appropriate actions of illegal contents and all OCSE related cases. In addition, IHC has run campaigns on raising awareness of online risks, and understanding of internet safety to children, parents/guardians, professionals and local communities. IHC works with partners and stakeholders to conduct research to gain knowledge and evidence based information to create an online learning/resource center towards eradicating OCSE.

**ChildSafe**[50]—ChildSafe is a movement of volunteer child-protection agents throughout Cambodian communities, which serve as the eyes and ears for a network of child-protection organizations throughout the country. Agents are trained to be aware of the situation of danger for children, and take action to protect them. ChildSafe works to protect children and youth those who are exposed to many abuses, from physical and emotional violence to sexual exploitation, forced labor and lack of access to education and health care. Children and youth served include victims of abuse, domestic violence, involved in the sex trade, school drop-outs or unemployed, using drugs, affected by HIV, migrants, in prison or in conflict with the law, and living on the margins of society.

**Child Helpline Cambodia (CHC)**[51] — Child Helpline Cambodia (1280), promotes child rights and build opportunities for children and youth protection through professional phone counseling, information service of appropriate partners. Through the consultation and giving information, so that CHC empower clients to make decisions and CHC only make intervene when the clients ask to do on behalf, and when it is an emergency, someone's life is at risk. CHC does not focus specifically on child sexual exploitation, but it provides a 24-hour, free hotline for children to speak with counsellors on a broad range of issues. While the mandate of the hotline is broad, counsellors also commonly receive reports on child sexual exploitation and violence, and are able to provide counselling, and outside service referrals as needed.

[49] Internet Hotline Cambodia. Accessed 17 Nov, 2018 from, https://www.internethotlinecambodia.org/
[50] ChildSafe Network. *The People.* Accessed 17 Nov, 2018 from, https://thinkchildsafe.org/the-people/
[51] Child Helpline Cambodia. *Organizational Overview,* Accessed 17 Nov, 2018 from, http://childhelpline.org.kh/about/organisational-overview/

# Chapter 2: Study Methods

This study assesses the current threat of OCSE in Cambodia, how it is manifest within Cambodian communities, where and how children are at risk, as well as the various capacities and gaps in national policy, legislation, criminal justice, social services, and the private sector in order to identify actionable, evidence-based recommendations for Cambodia-specific interventions. This assessment will be informed by the WePROTECT Model National Response (MNR) and drawing on learnings from local and international best practice.

The learning and mapping activities, as well as data within regional and international literature, indicate a notable gap in data from children and communities. The vast majority of data and case reports seem to come from regional and international law enforcement — often based on reporting from the National Center for Missing and Exploited Children (NCMEC). Most of these reports originate from child sexual abuse materials (CSAM) from electronic service providers such as Facebook, Google, and Microsoft. While these reports are important sources of actionable data, the do not give a complete picture of the landscape of OCSE risk in Cambodia, obscuring other forms of internet-mediated exploitation, which may be more prevalent in communities, such as grooming, sextortion, and live-streaming sexual abuse and exploitation. It is important that children are involved in helping us understand this broader landscape of risk at the local, end-user level. Thus, this study places a special emphasis on developing key data from children and their communities through learning workshops, built on the values of human-centered design.

The main objectives of this study are to engage with communities and key child-protection agents throughout Cambodia and the region for the purpose of:

- **Developing** a comprehensive and nuanced understanding of the nature and extent of OCSE in Cambodia at the community level, including an overview of key at-risk groups and key venues and platforms facilitating OCSE
- **Assessing and evaluating** the various child-protective capacities responsible for children in communities, including policy and governance, Internet service providers (ISPs), criminal justice, and media and communications.
- **Identifying** actionable and evidence-based recommendations for Cambodia-specific interventions, based on the WePROTECT Model National Response (MNR), which will feed into the development of an action plan to address OCSE in Cambodia
- **Building** the capacities of key local child protection agents in government and non-government sectors to understand and address OCSE at the community-level.

The study does not attempt to provide a representative sample of children across Cambodia, but rather aims to provide a rich, initial and qualitative picture of the OCSE in Cambodia, key themes and patterns of risk, as well as an assessment of the government structures in place to report and respond to cases and block/remove OCSE-related content online.

## 2.1 Sampling

This project will focus on gathering data from two key areas (see: figure 1):

**Children and their Communities:** This focuses on the understanding the experiences and perceived risks of children, their families, teachers, community social workers and law enforcement officials. Data is gathered through a series of custom-build centered learning workshops, co-created by social workers, child-protection specialists, and human-development centre. In addition, in-depth interviews were conducted at the community level with government,

law enforcement, social workers, key advocates from community-based organizations to add additional context for the data collected from the learning workshops.

**Child-Protection Capacities:** This focuses on building an understanding of the various capacities of national government, local private industry (ISPs), regional initiatives, and international child-protective mechanisms to protect children within Cambodian communities from the risks of OCSE. In particular, the study considers how these mechanisms do (or potentially could) work together to create a more integrated and responsive safety net and response mechanism to protect Cambodian children online. This includes conducting in-depth interviews with key government officials and representatives from internet service providers (ISPs), in addition to a systematic review of local and regional child-protection legislation related to OCSE, CSAM takedown and child-protection policies of Cambodian ISPs.

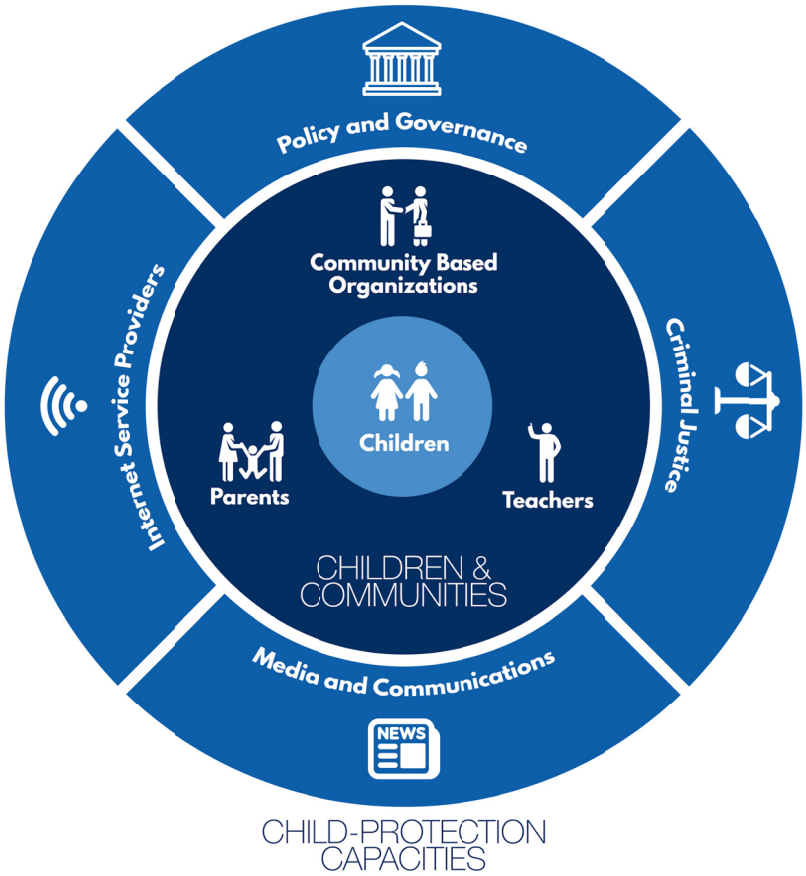



**Figure 1:** Model showing the two areas where data will be gathered in this study: Children and communities, and the surrounding child protection capacities.

# 2.2 Learning from Children in Communities

Learning workshops inform the core inquiry of this study into the nature of OCSE in Cambodian communities and explore the various forms of OCSE that experienced among children in Cambodia. The workshops provided a safe, interactive and creative environment for children to explore how they use the internet and what online risk looks like for Cambodian children. In particular, the workshops explored the various forms that OCSE is commonly manifest within the online environments of Children in Cambodia. Areas of exploration included the production and distribution of child sexual abuse material (CSAM), live-Streaming Sexual Exploitation

(LCSE), as well as numerous offline forms of exploitation, which may involve both online and offline components, such as the use of apps or other ICT platforms to meet children offline for abuse or exploitation.

The values of human-centered design guided the development and execution of the workshops. Thirteen learning workshops were conducted with 220 children aged 8-17 and 45 teachers from public schools, private schools, and NGO school centers in three areas of Cambodia: Sihanoukville, Siem Reap, and Phnom Penh (including Phnom metro areas in Takmao and Kandal province). These three areas were chosen because they are large metro areas and are the three areas which have the highest percentage of internet users in the country, according to national research conducted by LINREasia.[52] In addition, the presence of existing NGOs partners and other networks greatly facilitated the activities of the project. Separate Learning workshops were conducted with children from alternative (NGO) schools, public schools, and private schools in each local area. These groups were separated in order to provide a rough disaggregation of various socioeconomic groups in Cambodia. Lastly, three learning workshops with 45 school teachers throughout the three areas in order to develop a picture of teachers understanding and interaction with child protection in an online environment.

In addition to the learnings gathered from workshops with children and teachers in communities, a series of in-depth interviews were conducted in each local area with key government officials, representatives from ISPs, and social practitioners from community-based NGOs.

The common goals for the learning workshops were:

- To develop a comprehensive and nuanced understanding of the nature and extent of OCSE in Cambodian communities.
- To develop an understanding of who the key at-risk populations are and what makes them vulnerable.
- To identify the key venues, groups, and platforms that facilitate Children's vulnerabilities to exploitation online.
- To identify actionable and evidence-based recommendations for Cambodia-specific interventions.

The research partnered with four community-based organizations from Phnom Penh, Siem Reap, and Sihanoukville. In Phnom Penh, the research partnered with The Hard Places Community (HPC) and First-Step Cambodia (FSC). HPC is a social service provider that works with children from vulnerable communities in Phnom Penh with a particular focus on addressing issues of child sexual abuse and exploitation in communities. FSC is a specialist NGO project based in Phnom Penh, Cambodia, which provides a range of support services to boys and young men who are survivors of sexual abuse and exploitation. In Sihanoukville, the research partnered with social workers from M'lop Tapang (MT), which is a social service provider that offers a broad range of care and support for children from vulnerable communities in Sihanoukville including education, reintegration with families, life-skills training and creative and recreational activities, as well as response and protection from all forms of abuse. In Siem Reap, the research partnered with social workers from Terre Des Hommes-Netherlands (TdH-NL), which is an international development organization with project offices and social workers in Siem Reap that focuses on addressing sexual exploitation in travel and tourism (SECTT) by working with law enforcement official, support children' voice for advocacy, and protection of children from exploitation.

### 2.2.1 Human-Centered Research and Ethical Protocols

A four-day immersive training was provided to social workers and staff who came into contact with children. The training covered the philosophy and core values of human centered design

[52] LINREasia. (2018).

and ethical protocol for conducting research with children. This includes extensive and practical development of key skills, such as empathy, active listening, and designing a safe and fun environment where children feel important, heard, and able to safely talk about their "online worlds" ad the risks that they may face there. An important facet of this training was reinforcing the understanding that "children are the experts of their own realities" and the team, as researchers, were tasked with designing an environment in which allows children the space to communicate through art, words, and movement.

The training week included a brief orientation to the issue of OCSE as well as an introduction to the philosophy and approach of human-centered research. The team then focused on the building of specific skills related to human centered research— especially ethics, empathy, listening, communication, and relationship building. Following this, a full day was spent building an understanding and addressing the skills gaps of the individual participants and focus was placed on building the team's ability to work with one another throughout to build solutions to complex challenges. Toward the end of the training, the social workers worked with their teammates to create a day-long workshop that would best work for their own context. Then the research team used those separate concepts to build a unified day-long learning workshop to be used with children and teachers in Phnom Penh, Siem Reap, and Sihanoukville.

### 2.2.2 Review of Local and International Reporting Data on Cambodia

The research conducted a series of in-depth interviews with local and international OCSE reporting mechanisms, including the APLE internet hotline (Cambodia), Child Helpline Cambodia (Cambodia), National Centers for Missing and Exploited Children or NCMEC (United States), and the Interpol ICSE Database (International). Where available, the research collected and analyzed any current or historical data on Cambodian OCSE from these resources. Complete data was only available from APLE Internet Hotline, and Child Helpline Cambodia. The APLE internet Hotline provided data from a total of 204 OCSE-related cases over the past three years, and Child Helpline Cambodia provided data from a total of seven cases cases spanning the same time period. NCMEC provided basic metadata for more than 200,000 Cambodian reports of CSAM that have been referred to US Homeland Security within the past 5 years. Interpol was unable to provide specific Cambodian data on OCSE cases.

### 2.2.3 Online Surveys with Public School Youth

An online survey was conducted with 139 public school students connected with Family-Care First programming of Save the Children International (SCI) in Battambang province. The survey consisted of 30 questions which assessed how the youth connected to the internet and their thoughts and experiences related to internet safety and risk.

While it was the initial intention of the research was to collect a nationally-representative sampling of Cambodian youth in public, private, and alternative schools, due to time and political constraints, the breadth of survey was limited. The data represented in these surveys are in no way representative of the nation as a whole, however, it offers a useful set of learnings about internet use among this particular group of youth and provides potentially important comparison to the other learnings developed throughout this study. The findings of this survey are included as an annex in this report and are reflected upon within the study's main discussion and recommendations. It is our intention that future research initiatives will work with the Royal Government of Cambodia to build upon these limited findings and develop a nationally-representative of Cambodian youth in public, private, and vocational training programs.

# 2.3 Learnings on Child-Protective Capacities for OCSE

A series of in-depth interviews were conducted with key representatives from national, regional, and international law enforcement, government agencies, and child-protection organizations, as well as relevant members of the Cambodian private sector. The interviews assesses general awareness of OCSE and the various capacities to respond to the needs of children and collaborate with relevant partners and agencies prevent abuse and exploitation of children on the internet in Cambodia.

## 2.3.1 Criminal Justice

Criminal justice data is drawn from 9 representatives from national, regional, and international law enforcement agencies. In Cambodia, this includes, four members of Cambodian law enforcement agencies including Anti-trafficking police and the Cybercrime Unit, under the Ministry of Interior. In Thailand, the research draws data from one key representative of the Thai Department of Special Investigations and two key representatives of international law enforcement. Further, the research draws additional data from two key representatives from US Federal Bureau of Investigation (FBI) and Department of Homeland Security (HSI).

While the research followed many different lines of inquiry depending upon the agency and its capacity and function in responding to OCSE in Cambodia, interviews largely followed the following broad areas of inquiry:

1. What are the current practices and challenges for law enforcement in Cambodia, with regard to OCSE?
2. What are the current practices and challenges for the judiciary in Cambodia, with regard to OCSE?
3. What are the current capacity-building and training needs with regard to cybercrime and child protection?

During this process, the research also explored existing cases of OCSE that have been reported among police.

## 2.3.2 Policy and Governance

Primary data on policy and governance is drawn from 10 representatives from national and international governing and regulatory bodies. Nationally, this includes seven key representatives from Cambodian government, including the Ministry of Posts and Telecommunications (MPTC), the Telecommunications Regulator of Cambodia (TRC), and the Ministry of Social Affairs, Veterans and Youth Rehabilitation (MoSVY). Internationally, this includes, two key child-protection representatives from United National Children's Fund (UNICEF) and one from United Nations Office of Drugs and Crime (UNODC).

Some of the key questions guiding this inquiry are:

1. What is the nature, extent, and potential efficacy of regional (ASEAN) and national legislation and policies?
2. What opportunities exist within this context to comply with existing regional initiatives related to violence against children, and specifically online abuse and exploitation?
3. What are the key messages needed within this context for the development of education, awareness raising, and advocacy materials?

### 2.3.3 Child-protection agencies

Lines of inquiry with child-protection agencies varied greatly and largely depended upon the capacity and mandate of the organization being interviewed. For instance, interviews with organizations such as the National Center for Missing and Exploited Children (NCMEC) and the NetClean Project focused largely on the groups reporting and referral mechanisms established with local government and international law enforcement, while interviews with local child-protection agencies focused more on the issue of OCSE in Cambodia, victim identification and gaps in service provision.

Data was drawn from 25 representatives from national, regional, and international child-protection agencies. Among these are 12 representatives from Cambodian agencies including, ChildSafe, Save the Children International, Kalyan Mith, M'lop Tapang, Women's Resource Cambodia, Angkor Hospital for Children, Child Helpline Cambodia, and Action Pour Les Enfants (APLE).

### 2.3.4 Private Industry

The research also conducted two in-depth interviews with two representatives from two Cambodian Internet Service Providers, which were broadly directed by the following lines of inquiry:

1. What are the current mechanisms, attitudes, commitment, motivation, and capacity of ISPs to better protect Cambodian children from OCSE?
2. What responses exist within the current ICT ecosystem – including ISP's connection with APLE Internet Hotline, blocking and removing access to OCSE contents, and industry engagement?
3. What are the key messages needed for the development of effective reporting, education, awareness raising, and advocacy materials?

# Chapter 3: Children's Experiences Online

## 3.1 Learning Workshops

### 3.1.1 Understanding the Online Environments of Cambodian Youth

Youth were encouraged to think broadly about the ways in which they experience the internet, including how they connect, where they connect, and what they internet world might look like if they were able to 'step inside' of it and walk around. As a means of doing this, children in each learning workshop spent a half-day working together in small groups of 4-5 people creating large interactive maps of their "internet worlds". Facilitators joined with each group of youth to ask probing questions in order to keep the exploration of their internet world interactive, exploratory, and fun. The children's internet maps included all of the places on the internet that they like to spend their time, why they like it, and what types of people they find there, and what activities they like to do in each of these areas.

Youth reported spending a great deal more time on the internet and described a much more diverse range of internet access points than anticipated. Children from vulnerable communities also demonstrated an especially detailed awareness of a variety of unsecured access points for free-wifi within their communities, including TukTuks, hotels, barber shops, and busses. Time spent on the internet ranged greatly among children in learning workshops with children reporting 15 minutes a day to five children who reporting spending nearly every waking hour on the internet. Youth from private and public schools indicated using internet for slightly longer hours, on average, in comparison with youth from vulnerable communities (5.8 hours v 4.8 hours a day). Overall, among the 148 children providing responses, 60 or 40% cite spending about 1-2 hours on the internet, 38 or 25% cite spending 2-4 hours, 28 or 19% cite spending 4-6 hours, 12 or 8% cite spending 6-8 hours, and 10 children or 7% cite spending more than 8 hours a day on the internet.

#### 3.1.1.1 Child Sexual Abuse Materials

More than one in four groups, or 16 of the 58 (27%) groups of children and teachers, describe the solicitation, distribution, or production of Child Sexual Abuse Material (CSAM) as a key risk within their online environment. While no teachers were aware of CSAM as a key risk, this was a common area of discussion among children in all areas that workshops were conducted. CSAM was primarily discussed as being send and received through Facebook (50%) or through Messenger (40%), which is a part of Facebook. Perceived risk of CSAM seem to be diverse and often involves other forms of OCSE as well, including extortion and live streaming sexual content. One child from an NGO school in Takmao note, "Some friends in Facebook have sent nude photos, pornographic videos in messenger. Some girls who want to be popular online have tried to (do) live videos to show their bodies." Further, there is some indication of potential grooming of youth to produce CSAM in exchange for money. One child from a public school in Siem Reap cites, "Bad people use Facebook for grooming young people, promising to give money, material (items) and young people can do whatever they are told".

#### 3.1.1.2 Live-streaming of Sexual Content

One in four groups, or 14 (24.1%) perceive various forms of live streaming sexual content to be a key risk for children. The majority of awareness of risk involves youth using the app Bigo Live (57%), as well as Facebook and Messenger. Youth describe live-streaming sexually explicit or sexually provocative content, often at the request of other users. In other instances, youth are cited to use sexuality to market products for sale through online platforms. One girl in Siem Reap describes, "Bigo Live has been used by many girls and women who want to sell cosmetic products. (They) always live-stream and show their bodies which makes youth feel sexual"

Some youth indicate that this happens as a way of earning money or gaining more followers, while other cases indicate children being groomed to participate in such content. One public school student from Siem Reap cites, “Both Apps (Facebook and Messenger) have been used by bad people to groom (young) people and request them to send nude photos, video livestream. Sometimes, they (will) make a date and (be) raped.”

### 3.1.1.3 Grooming for CSEA

More than one-fourth, or 16 groups (28%), describe grooming as a significant online risk. The majority of youth and teachers who specifically perceive grooming as a risk seem to be from the Sihanoukville area. However, grooming is often a part of (and may not always be outrightly mentioned) in a variety of other OCSE-related offenses described in other areas as well. For instance, many children describe risk of adults sharing pornographic images with them, which could also be a form of grooming. Grooming is described to happen in a diverse number of ways and in a diverse number of contexts. The vast majority of grooming described is cited to happen on Messenger, however, other apps such as Bigo Live, Instagram, and WeChat are mentioned as well. One public school student from Siem Reap cites, “Bad people have used Facebook for grooming young people (promising) to give money, (and other) materials, so that the young people will do whatever they tell them (to do).”

### 3.1.1.4 Distribution of Pornography to Children

The distribution of pornographic materials from adults to children (and also among children) seems to be common and described as a known risk by the majority (35 or 60.3%) of groups. Some children cite receiving pornographic materials from adults that are directed specifically at them, seemingly for the purpose of grooming or receiving sexual images from the child in return. In other cases, children describe being added to Facebook or Messenger groups where pornographic images are regularly posted and exchanged. One child recounts, “someone sent me three nude photos through Messenger. I get angry with people (like this). I’m just a little girl, maybe they think I am a prostitute.” While some children indicate rejecting or deleting the images and blocking the sender, children cite other youth who distribute the images further or contribute some of their own.

In addition to being sent pornographic images directly, children also describe commonly seeing pornographic images through third-party advertisements in various apps including Facebook, Youtube, and online games. One child cites, "when I scroll through my Facebook page feed I saw a video livestream of a girl taking off (her) clothes and announcing to sell her body for sex". Another describes that he often sees pornographic videos and images appear on the screen from third-party advertisers while he watches cartoons.

### 3.1.1.5 Extortion

Various forms of extortion through Facebook, Messenger, and other apps were described as a key risk in more than one-fourth, or 15 of 58 groups (26%) of children and teachers. Examples of extortion were diverse and seemed to be committed by a variety of actors and for a variety of different reasons. In some cases, perpetrators groom victims to share sexual images of themselves and then used those images as blackmail to extort money from the victim, other children describe users who hack into their social media accounts in order to pose as a family member of the victim and request money. In some cases, perpetrators are described to use public or non-pornographic images of the child and edit them to appear as though the child is doing something sexual. Those pictures are then be used as a form of blackmail to extort money from the child or to get them to perform other requests for the perpetrator. One public school student from Siem Reap notes, “some people use their Facebook account to find online friends and groom them to do (a sexual video call) and then take a screenshot. Then they send a message to threaten victim to pay money.”

## 3.1.2 Assessing High-Risk Platforms

### 3.1.2.1 Social Media Platforms

**Facebook** is cited as a high-risk platform by 47 of the 58 groups (81.0%) of children and teachers. Some of the most common risks include seeing or receiving unsolicited adult pornography (47%), receiving sexual images of children or children being asked to send sexual images (21%), as well as various forms of extortion or threats (21%)— often through the use of embarrassing sexual images featuring the child, or the child's likeness, in addition to other risks.

**Pornography**: Posting or sharing pornographic images is the most commonly-cited risk on Facebook with 22 of the 47 groups describing this as a risk. One child cites, "I have seen a lot of pornographic images (that) have been posted on Facebook. I think adults have sent all these images and they have sent it to many (other) people too." In other instances, pornographic images are described to be specifically, by adults, to the walls of children.

**CSAM**: The creation and distribution of Child Sexual Abuse Material was also a prevalent risk discussed by more than one-in-five (10 of 47) groups, which identified Facebook as a risky app. This includes the sharing of sexual images of children, adults and children requesting other children to send sexual images and content, as well as "live-streaming" sexual performances. One boy from Siem Reap cites, "(Facebook has) been used by bad people to grooming some people (youth) and requesting them to send nude photos, live-streaming (sexual) videos. Sometimes, (users) make a date and rape (others)." In addition, various forms of extortion using sexual images of children are indicated, which will be discussed further below.

**Extortion**: Various forms of extortion were also recognized as common risks on Facebook by 10 of the 47 groups of youth and teachers, which identified Facebook as a risky app. This theme was diverse, but commonly involved 'hackers' or persons able to access the child's Facebook account in order to extort money from friends and family of the child. One child describes a hacker who was able to convince the child's relative that his mother had become ill, tricking them into sending money. In many cases, this did not involve hacking into the child's account, but rather using photo-editing software to change public pictures of the child to appear as though he or she were nude or performing sexual acts. In other cases, actual nude or sexual pictures of the child were obtained and were then used to extort the child into either providing services, more images, or money to the person making the threats.

**Instagram** is cited as a risky app by 10 of the 58 groups (17.24%) of children and teachers, predominantly because of sexual or pornographic content that is commonly shared through the app. Some groups describe sexual content from other live streaming apps (described below) will be uploaded to instagram or other similar social media platforms where the content-creators sexual images can be shared to a wider audience, without their knowledge. Another group cites instagram to bear much of the same risks as found on Facebook, as the platform provides both a place for users to display personal information along with a messaging feature for users to have private conversations with other users.

### 3.1.2.2 Communication Platforms

**Messenger** is cited as a high-risk app by 42 of the 58 groups (72.4%) of children and teachers. Children consistently describe a key safety concern on Messenger in which strangers that they have added on Facebook are able to send them a "wave" icon. While users who are not connected on Facebook are usually not able to send unsolicited pictures or video to one another. If the child replies to the "wave", the ability to send photos, videos, or to start an audio or video call are automatically unlocked, allowing the stranger to potentially send explicit content, connect with the child through a webcam, or send links to other explicit or malicious content. Further, children can be added to existing messenger groups without their consent, by anyone who is connected with them on Facebook. This allows any Facebook user within the child's network of friends to potentially add them to messenger groups were explicit materials

are being exchanged, allowing potential perpetrators (who may also be in the group) to have direct access to children online.

Some of the most common risks include seeing or receiving unsolicited adult pornography (45%) and the potential grooming of children for sexual abuse, which includes sending sexual images of themselves (26%). Related to grooming, are various instances where children were encouraged or asked to share sexual images of themselves (CSAM), which is described in eight or 19% of groups citing Messenger as a risky app. Messenger is cited to be used as a tool for extortion or scams in six or 14% of cases. Differentiating between risk categories here is difficult as many of them overlap or are interrelated with one another. For instance, while 19 groups cite risks of receiving unsolicited pornographic materials, many of the instances of grooming described by children on Messenger also involve the exchange of unwanted sexual content, which may not necessarily be considered as pornography. Further, some of the instances of CSAM also involve the perpetrator first sending alleged sexually-oriented images of him or herself, in order illicit sexual images from the child in return, which could be a form of either grooming and pornography. In view of this, it should be considered that there are numerous overlapping themes within the categories defined below.

**Pornography**: Nineteen of the 42 groups indicating Messenger as 'risky' (45%), indicate various instance in which children or their peers have received pornography— mostly from strangers on the internet. Children cite that some strangers will add them as a friend on Facebook, while others will include children on an existing Messenger group (with many users), in which users will send and distribute sexual content in a private and encrypted messenger group. One boy describes the issue of fraudulent messages, where a user with a young female will be displayed in the profile picture and send sexual images, then after chatting and requesting a live video call the user will find a man on the other end of the call. In particular, a number of children describe this happening with "indian" perpetrators— which may not specifically denote someone from the country of India, but could potentially refer to a range of persons of Middle Eastern or South Asian descent.

**Grooming:** Eleven groups (26.19%) describe various scenarios on Messenger in which strangers will attempt to build relationships with children in order to exchange sexual images or for other illicit activities. A number of children describe unknown adults who will add them on Messenger and attempt to befriend them. In some instances, the adults will have profile information, including images, that make them appear to be younger or as if they are also a child. In most of these instances, the adult will try to start a conversation with the child, often sending adult pornography or sexual images of other children attempting to make the child participate by sending their own sexual images in exchange. In most cases, it is unclear if the perpetrators are foreign or Khmer, however, in three cases where video contact was made between the child and perpetrator, children recall seeing a foreign adult on the other end of the call. One child describes, "a foreigner sent a nude photo after video calling me. But I blocked his account. After that, he sent a friend request to me again but I did not accept him." In addition, the child cites that the same account attemped to make similar contact with this friends.

**CSAM**: Eight groups (19%) describe Messenger as a platform where Child Sexual Abuse Materials are produced and distributed. In some instances, perpetrators seem to be eliciting sexual images of children in order to extort money from the child by threatening to post the images publically (sextortion). One public school student in Siem Reap describes, "Some people use their Facebook account to find online friends and groom them to do (a sexual video call) and then take a screenshot. Then she/he sends a message to threaten the victim to pay money." In other instances, images seem to be elicited for sexual interest, however the details are not clear from the children's descriptions given in this activity. More detailed accounts will be explored in the sections below.

**Sextortion and scams**: One in six groups (16.66%) describe Messenger as a risky platform due to various types of scams and extortion, including the use of sexual images of children to

extort money or other illicit favors from users. In particular, a number of children describe people editing their public images from Facebook to appear that the child is naked or committing sexually explicit acts. The perpetrator will then require the child to provide money or provide other favors in exchange for the images not being released. With regard to scams, some perpetrators will promise to send a package or money, however the user needs to pay a fee to receive it, among other instances.

**Line** is described as a risky app by 14 of the 58 groups of children and teachers (24.13%). Children in learning workshops gave little specific information about what makes Line a risky app, but seemed to group Line as having many of the same risks indicated within other communications apps. Children indicated Line as a route through which they could receive sexual images and privately come in contact with strangers met through other online platforms, such as Facebook, Rules of Survival, and TikTok.

**Skype** is described as a risky app by six groups of children and teachers (10.3%). Similar to Line, little specific information was given with regard to what makes Skype risky, but larger discussions surrounding this, and apps like this, indicated Skype as having many of the same risks, including as a route through which children could receive sexual images and privately come in contact with strangers met through other online platforms.

#### 3.1.2.3 Gaming Platforms

In general, many gaming platforms were identified as high-risk online environments. Despite this, few risks were indicated that are directly related to OCSE on the platforms themselves, however, broader conversations on online risk indicate online gaming platforms to be key communities in which potential perpetrators of OCSE will make initial contact with children. Perpetrators are then able to find children on Facebook or other platforms by requesting their information in the game, or by using the child's public screen name within the game to find the child on another online platform where further contact can be made. Some notable risky gaming platforms discussed by children are addressed below.

**Rules of Survival** is a free-to-play, multiplayer online battle game which allows its 150 million registered users from around the world to compete against each other. This game is described as a high-risk game by 29 groups (50.0%). Three groups (two of children and one of teachers) describe a variety of privacy concerns, citing that perpetrators are able to meet children through the game or gain access to their facebook information, allowing them to contact the children on other platforms. One child cites, "Rule of Survivor is an online game which allows us to play with other groups of players. We can talk (to them) online and sometimes group members request our phone numbers or Facebook accounts." Apart from this, the majority of risk understood by children within this game were related to interpersonal disputes between players, which was cited by 11 groups (38%) of children. Beyond this, children— particularly those from vulnerable communities— cite that this is a risky app because many of the games features require users to pay money (discussed by six groups or 21% of those seeing the app as risky). Because of this, users spend money that they don't have, are cited to borrow money from other children or take money from their parents.

**AK2**, also known as "Mission Against Terror", is a multiplayer, free-to-play, first-person shooter game, which is similar to commercial games such as Counter-Strike or Call of Duty. This game is described as a high-risk game by 15 groups (25.86%). Only one group of children indicated concerns for their privacy. One child cites, "sometimes, when we are playing the game (other users) can take our picture and share it with others." Another group cites that, apart from these, few risks were directly related to OCSE but were rather associated with other issues, including the cost of the game and interpersonal disputes between players.

**PUBG**, also known as "Player Unknown's Battlegrounds," is an online multiplayer battle-game by PUBG Corporation, a subsidiary of Blueholecited, a South Korean video game company. This game is described as risky by 15 groups (25.8%). The primary risks identified by children

were interpersonal disputes between players and some users who would curse or insult children while online, as well as fighting in real life with other youth because of gameplay. Another key concern discussed was the ability of other anonymous players to chat with children during gameplay. Two groups discuss personal experiences of youth meeting up in real life with anonymous persons who they had met in the game. One child recalls, "PubG has introduced us (to) many online friends. These friends have sometimes asked us to meet in real life and tried to get us to join their gang."

**GTA 5,** also known as Grand Theft Auto 5, is an action-adventure video game in which players control three lead protagonists throughout an urban environment to complete various, often explicit, missions. This game is cited as risky by 8 groups (13.8%). The majority of children (eight of the five groups) using this game cite that it is risky due to the intense violence and sexual content, which is pervasive throughout the game. Beyond this, one group cites the game is risky due to scams, citing an instance in which one player had attempted to get financial information from another player.

### 3.1.2.4 Live-streaming Platforms

Live streaming is the broadcasting of real-time, live video from a computer or mobile device to an audience on the internet. This phenomenon has become increasingly appealing to children and young people in recent years as it presents the chance for them to be a creator and presenter and be seen by an audience around the world. Anyone with the app can be a live presenter and can broadcast anything that are doing across the world in real-time. User interaction with their audience is a major component of these platforms. This happens through public chat rooms which operate within or alongside of the video broadcast. This gives both the presenter and their audience the ability to talk or, in some cases, send digital gifts that can be exchanged as monetary credit. Within the learning workshops, TikTok and Bigo Live were the two most popular live streaming apps discussed by participants and both were commonly identified as high-risk apps.

**TikTok** (formerly known as musical.ly) is a social media platform for creating, sharing and discovering short music videos. Users are able to create short music videos with the tools on the app and share them with other TikTok users. This app is described as risky by 25 of 58 groups of children and teachers (43.10%). Sexual content was the most commonly identified risk on TikTok (seven groups or 30%) with most groups citing sexually-oriented content produced by presenters on the platform (including some who are cited to appear very young). Two groups (8.69%) describe overly sexual content on the app including nudity and users who use the platform to earn money for such content. Other groups cite other risks presented on the platform including youth who learn sexual or other inappropriate language and behaviors.

**Bigo Live** is a live streaming app that is a platform to allow users to stream their live, video, host show and interact with other users. An interesting feature of this app is its ability to be monetized. Users purchase bean packages to "gift" or tip their favorite vloggers. Vloggers are then able to cash out their in-app currency for real world cash. Bigo Live is described as risky by 17 groups (29.3%). While Bigo Live is discuss by fewer groups in comparison to TikTok, the risks described by both teachers and children are notably more severe. Eight of the 17 groups (47.05%) that cite Bigo Live as a risky app describe witnessing live sexual content featuring both children and young adults— including many who provide such content in exchange for payment and some who will then agree to meet with members of their audience privately on other apps. One public school student in Sihanoukville notes, "Bigo Live is mostly used by (girls selling sex). They live stream (and show) their bodies and talk about sex and give their contact information."

YouTube was cited as risky by 15 of the 58 groups of children and teachers (27.6%). The majority of groups discussing YouTube (62.50%) identify the widespread presence of pornography to be a key risk for children. Several groups of both teachers and children highlight the connection between having easy access to pornographic materials and sexually harmful

behaviors among children and youth. One public school student from Siem Reap cites, "after someone watches pornographic videos on youtube, they would like to practice (what they have seen) in real society." Another male from a vulnerable community in Phnom Penh describes some of the impacts that he has noticed within this own context. He notes, "Sex videos have influenced children to practice sexual abuse to others. For example, it has influenced to children to have sex (at an) early age, (and) secretly look at other people when they are taking a shower. The sex videos affect our brains", he cites.

### 3.1.3 Online Risk Storyboarding

After mapping our their online environments and participation in other activities aimed at identifying and analysing key OCSE risks, children were asked to build a story of how something like OCSE has, or potentially could, happen within their online environments. Among the 220 children across 13 workshops, 117 shared specific narrative examples internet-related risks in their online environments. Some children shared hypothetical scenarios based upon their knowledge and experience with the apps that they most commonly use, while others developed real stories from incidents that have happened to them personally or to people that they know.

Seventy-one of the 117 children (60%) shared examples of Online Child Sexual Exploitation[53] within their online environment. The vast majority, or 59 of the 71 (83%), shared either personal experiences or second-hand accounts of OCSE. More than half of these, 37 children or 53%, shared personal experiences of OCSE and nearly a third, 22 or 31%, second-hand accounts of OCSE that had happened to someone that they know. This means that, out of the 220 children involved in the learning workshops, 37 or 17% (about one-in-six children), shared a personal experience of OCSE-related risk on the internet. Thirteen accounts were either hypothetical or reflected something that the child had read in the news and the remaining accounts were unclear.

**Grooming**: Among the 117 children who shared stories of online risk, 29 children (25%) shared various personal experiences (18 accounts) or second-hand experiences (11 accounts) of grooming or sexual advances by adults online. Most experiences of grooming were cited to have taken place through Facebook and its messaging app (20 accounts), as well as other messaging apps, such as Line. The targets of grooming were described as both males (11 accounts) and females (14 accounts), as well as four accounts in which a gender was not specified. Offenders were largely described as adult males (20 accounts), several of whom were believed to be of foreign nationality— especially Indian[54]. In many accounts, children describe receiving friend requests or direct messages from an unknown person on Facebook, who will attempt to start conversations with the children and build rapport. In some instances, the unknown person is described as starting live video calls with the children, or directly sending explicit pictures, and in some cases, requesting explicit pictures from the children in return. A girl from Sihanoukville describes a man who added her on Messenger and began chatting with her. She cites, "*he (began) sending me pornographic pictures of both men and women. I clicked to open the pictures, but I suddenly got angry with him that he sent me such kinds of pictures. I supposed that wanted to have a sexual encounter with me. I blocked him from my account and deleted all the pictures that he sent to me.*" In another instance, a girl from Sihanoukville describes a previously ongoing incident in which a Chinese male who she did not know and was not added as a Facebook friend. She recounts that the man would regularly try to chat with her on Messenger, send her explicit photos and videos, and ask to meet up. She

[53] Examples specifically related to Online Child Sexual Exploitation. Many children came up with stories which involved various offline risks to violence or exploitation, including phone and text message scams and various forms of violence and exploitation within internet cafes (especially among children from vulnerable communities). However, these examples were excluded because they did not seem to be specifically related to OCSE.

[54] While children described a number of offenders as "Indian", it is unclear if this is, in fact, the nationality of the people described. It should be noted that "Indian" could also be commonly used as a broad ethnic term for many groups of people of South Asian and Middle Eastern descent.

cites, "*After I searched his profile, (I found that) he is a Chinese man and he has posted many pornographic images and videos which showed nude women. He is a bad man who wants to groom us to work in prostitution.*" Following the workshop, the child was provided with needed resources to stay safe on the internet and the case was further addressed by local social workers working closely with the project.

**Receiving pornography**: Children commonly describe situations in which they receive or are exposed to pornographic videos and content against their will. One-in-five of the 117 children (23 or 23%) describe a diverse range of scenarios where adults, other children, and online advertising exposes them to various kinds of explicit pornographic materials online. There is also some overlap here with accounts of grooming, as adults are commonly cited (by children) to use pornographic pictures and videos as a means of grooming children to share or participate in sexual activities and content. Of the 23 accounts shared by children, 16 were cited to have taken place on Facebook or its messaging app, two are cited to have taken place on other unnamed messaging apps, one takes place on Line (a messaging app) and another takes place on TikTok (a social media app), while three accounts do not specify a particular app or platform. The majority of accounts (17 of 23) are described as personal experiences of the children, while six accounts are described as something that happened to someone the child knows. Some children describe being added to Facebook or messaging groups, without their request or consent, where pornographic images or videos are commonly shared among users. In other instances, children commonly cite being brought into explicit messaging groups, without their consent, and receiving pornographic videos and images. This was also a notable theme that emerged from the ecological mapping activities as well. One child recalls, "Once, I joined in a group chat and one group member sent pornographic images of a man and woman. After I saw it, I left the group. I think the images were not good (to see)."

**Live-streaming**: Five accounts from children describe various instances that were consistent with Live Online Child Sexual Abuse. Three of these cases are described to have taken place on Facebook or its messaging app, one is cited to have happened through the app TikTok, and another account does not provide details of the online platform. Three accounts involved children who were directly targeted for sexual acts by adults using a webcam. In another case, a 14 year old boy from Siem Reap describes being targeted by a foreign male while using Facebook messenger. He cites, "An Indian guy added me on messenger and started a video call. He showed (me that) he has taken off his clothes, while he was chatting with me. He sometimes sent messages in English, and Khmer to me. I blocked him in my messenger, but later, he appeared again to chat with me. I think he might (have) wanted me to do the same as he did."

In one case a child and her friends were approached on the street to be filmed for sexual activities that would be live streamed on the internet. A girl from Siem Reap cites, "near the nightclub and karaoke, a stranger came to us and asked if we can wear a sexy short blouse and pants and dance for livestream video?" She cites that the stranger continued to ask for personal information about her, her friends, and her family.

**CSAM**: Six children (5%) describe instances in which they (or other children that they know) have had sexual images of themselves taken and/or circulated on the internet. Four of the six accounts involve the production of CSAM in an offline environment and uploading the images to an online platform, while the other two accounts involve the distribution of existing explicit images of a child to an online forum. Three accounts are described as taking place on Facebook and/or its messaging app, and the other three accounts do not specify the online platform. In two of these accounts (one a personal experience and the other from third party experience), a child was offered money by an adult to have their pictures taken. One male from a vulnerable community in Phnom Penh describes, "I met a man (in a particular location) while my friends and I were playing online games. He has a big black camera and requested us to take nude photos (in exchange for) 5,000 KHR. One of my friends agreed to take a picture, but the other two did not." One account involves elements of bullying and harmful sexual behavior.

In this account, an older youth (19 years old) is described as making fun of a younger boy for his body size and proceeded to force the younger boy to pose for a picture without his clothes on. These pictures were then circulated on Facebook for the purpose of belittling the younger boy. While this account does not seem to be overtly sexual in nature, the abuse and damaging implications for the child are significant.

Accounts of the production and distribution of CSAM were represented in all areas (Phnom Penh, Siem Reap, and Sihanoukville) and were described solely by children from vulnerable communities. It should be noted, however, that while no accounts of the production or distribution of CSAM were described by public and private school students, all groups of children indicated notable risk and it should not be assumed public and private school students are less at risk. Five of the six accounts were second-hand, and cited as something that happened to another child that they knew. One account was described as a personal experience.

**Youth-Generated Sexual Images**: In four accounts, children give second-hand accounts of boyfriends and girlfriends who keep intimate or sexually explicit images of one another. In two of the accounts, sexually explicit images of children were posted publicly to Facebook, as a means of revenge after the couple has a dispute or ended the relationship. In another account, a girl is cited to have met another child online and formed a romantic friendship. The girl is eventually convinced to share sexually explicit images of herself with the other child, who threatens then to repost the images unless the girl is able to pay 50,000 Riel (about $12.50 USD).

### 3.1.4 Socio-economic Considerations

While OCSE-related experiences were described by children in all locations and among all economic groups (public schools, private schools, and children from vulnerable communities), there were some unique vulnerabilities that seemed to emerge among children from vulnerable communities. While these groups represent the majority of children in learning workshops, they seem to demonstrate a broader range of vulnerabilities to OCSE and OCSE-related experiences were more commonly disclosed among these groups, in comparison with children from public and private schools. It should be noted, however, that the learning workshops are intended to provide a qualitative view of some of the themes and patterns of OCSE-related risk among children and in no way are a means of assessing prevalence. Still, slightly more than one-in-four youth from vulnerable communities, 23 or 26%, describe various experiences of grooming on the internet. This is more common than what was found among children from public and private schools, where slightly more than one-in-six children described the same. Receiving pornographic images from unknown adults was also common, described among one-in-five children from vulnerable communities.

In addition to risks specifically on the internet, children from vulnerable communities also indicate greater awareness and experiences of environmental risks, while they access the internet. This is notable among street-involved youth, who commonly use public internet cafes to access the internet. Environmental risks included violence from other users, being exposed to pornography and other adult sexual activities in the cafes themselves, being robbed by other children, as well as physical violence from owners and other youth. While this is not specifically related to OCSE, this was a prevalent discussion among such groups, and poses great potential risks to children and young people.

While children from public and private schools gave fewer specific OCSE-related accounts, they were very aware of the existence of OCSE related risks within their online environments, including adults who attempt to groom children for sexual abuse, live-streaming sexual exploitation, extortion, among others. Only 10 of 23 children from public and private school provided specific OSCE-related accounts risk on the internet. Among these 10 accounts, four (17% of all public or private school children) indicate various experiences of grooming on the

internet. Three of the four accounts are personal experiences and two are second hand. Three youth (13% of public or private school children) describe various instances of receiving pornography from adults. One child recounts a story of his classmate who had received messages from a person in another country. This person asked him for his personal information, but the classmate denied. Later, the person began sending the classmate pornograpic images through Messenger, prompting the classmate to block the user's account. Youth-generated sexual images is described among two of the 10 children from public or private schools, along with two account of extortion using sexually explicit images gained from users.

## 3.1.5 What is Needed for A Safer Internet

At the end of each learning workshop, students and teachers were asked to return to their small groups and imagine how, if they were given unlimited powers, they would make the internet 100% safe for young people in Cambodia. Ten small groups of teachers and 47 small groups of children brainstormed solutions that they felt would make their online worlds safer. Overall, teachers tended to discuss the internet in broader terms of danger, addiction, and isolation from family, while children were, overall, more likely to see the internet as a largely positive environment, which also contained real dangers that needed addressing. Teachers were more likely to suggest various ways of blocking access to the internet itself and providing books in its place, while students tended to take a more nuanced approach, seeing solutions in advocacy, awareness, and blocking specific content and accounts that posed risks to their safety.

### 3.1.5.1 Teachers Perspectives

Teachers tended to see the internet as something that negatively influences children to skip class, come late to class, and to be less attentive in their studies. Many teachers used the language of addition in describing their students usage of social media and mobile devices. Teachers' groups tended to take more time to consider the negative impacts that they internet had on the health and wellbeing of their students, citing changing behaviors and isolation, and lack of social connection among children who had an addiction to games and social media. While teachers focus more on the internet and ICT devices themselves, kids focused more on concerns about specific dangers online and exploitation issues within their online environments. While teachers cited internet addiction as a key concern, they estimated children to spend less time online than children estimated for themselves.

In considering solutions to make the internet safer for children, teachers were more likely to suggest various ways of blocking access to the internet itself and providing books in its place, while students took a more nuanced approach, seeing solutions in blocking specific content and accounts which posed risks to their safety. Their solutions included the following:

**User Awareness:** Teachers believed that children should be made aware of the dangers of the internet and trained in ways of staying safe. They cite that this should include training on how to use social media privacy settings to keep their pictures and personal information safe, how to set a strong password to protect users' accounts, and how to understand and avoid the practices of online predators. Awareness raising should also be conducted within families and local communities, including students, teachers, parents/guardians, social workers, family, police, local authorities, NGOs and institutions which work with children. All of these groups should know how to report child-protection issues through helplines such as ChildSafe, Child Helpline Cambodia, and the APLE Internet Hotline.

**Greater parental involvement and control**: Teachers indicate that parents should play a more active role in monitoring their children's use of internet-connected devices. Parents should know how to engage 'safe browsing mode' on YouTube and Internet Browsers and parents should set boundaries and time limitations to kids internet access so that kids can have more time for their studies. Teachers believe that the internet has a negative impact on the socialisation of children, citing disrespect for adults and the use of bad language. One teacher

in Siem Reap cites, “Some game players have said dirty words (related to sex) in video.” Another teacher in Sihanoukville states, “Children have become addicted to TikTok (and) always ignore adults and use bad words just as they are used on (the app).” Further, they cite that children under the age of 17 should not be allowed to have their own personal internet-connected devices.

**School Internet Policies:** Teachers believe that the internet is too easily accessible to children and has a negative impact on their studies. In particular, teachers indicate issues with using smartphones in the classroom, which distract children from the curriculum. In addition, teachers cite concern over the close proximity of internet shops to schools, citing that some students will walk to nearby internet shops instead of attending classes. Teachers suggest that the Ministry of Youth, Education, and Sport (MoYES) should release a memo to restrict internet use in schools, and forbid internet shops from opening within 500m of the school property. Additionally, teachers request specific age restrictions for internet shops to prevent children from playing games and accessing the internet without supervision.

**Libraries as alternatives:** In place of ICT devices, several teachers groups suggest that public and school libraries should be provided to encourage students to study through reading books, so that children would spend less time on the internet.

### 3.1.5.2 Student’s Perspectives

Children are much more able to engage with the topic of specific online risks and dangers and are able to provide more nuanced solutions to the issue of OCSE in comparison with teachers. In particular, children are able to discuss specific potential harms that they face from adults who send them pornography/sexual content, grooming, cyberbullying from peers, online extortion, and the effects of adult content on children. Children also raise concerns regarding online privacy and the sharing of their personal data with strangers, especially in online gaming environments. Children indicate a much broader and more nuanced understanding of internet devices, ISPs, apps, and internet platforms in comparison with their teachers. Children demonstrating a deeper understanding of internet safety, including knowing how to block friends and delete or block particular content.

While teachers tended to see the internet and ICT devices as being counter-productive for school and in competition for students’ attention, children indicate regularly using the internet for school, research, and other forms of productivity, including learning new skills, personal research, and applying for scholarships. In contrast, teachers did not greatly express any positive capacities of the internet, or indicate using the internet for productivity or self-development beyond the use social media to read the news and looking up basic information.

**Potential Solutions**:

**User awareness:** Children underscore the importance of their peers and family members to learn about the online environments of children. They indicate a specific need for awareness-raising on internet use and safety within their communities, including among family members, neighbors, and peers and for training on what different apps and games are, where dangers lie, and how to keep children safe online. In particular, children describe the need for children and parents to know how to better protect their personal information online, how to create strong passwords, and better utilize app privacy settings. Children suggest the development of public awareness campaigns for TV and within schools are needed to communicate potential dangers online and how people can protect themselves from hackers and other predators on the internet.

**Advocacy and awareness education for online safety**: Children also stress the importance of knowing how to avoid strangers online. Children note that their peers need better awareness of based online safety, including messages about not adding contacts or accepting a friend request from people that they do not know and not reply to messages, posts, or pictures sent by

anyone that they do not know personally. Children stress the need for their peers to understand the importance of not trusting the people that they need online, even if they have mutual Facebook friends. They cite the importance of carefully reviewing profile to be sure that the account really belongs to the person pictured, and not an imposter. Further, children stress that their peers need to understand the dangers of posting 'sexy photos' and to avoid live-streaming (video) sites and apps, as well as sites that contain pornographic videos and images.

**Report dangerous content/situations:** Children and their parents should know how to report risky or abusive content to social media platforms, so that appropriate actions can be taken against the accounts that misuse social media. Children also suggest that social media and gaming companies (especially Facebook) should be more active in screening users and responding to content reporting to make sure that children stay safe while they are online. In addition, children cite the importance of knowing local resources to report abuse, such as the Child Helpline Cambodia (1280). They indicate that services like this are important because they provide social workers which can trust to protect their privacy and find solutions by discussing issues with people who can help.

**Environmental Risk Mitigation:** Children also acknowledge significant environmental risks of accessing the internet through public internet cafes and cite that public internet cafes should not be located near schools. While teachers seem to cite issues of children skipping class to go to internet cafes, children recognized not only this risk but also significant environmental risks within the internet cafes, themselves, including violence, and exposure to other adults who access pornographic content on public computers and, in some cases, perform lude or inappropriate activities in the presence or vicinity of children.

### 3.1.5.3 The Concept of Assessing

The learning workshops demonstrate a great generational divide between teachers and students, not just in terms of their ability to use the internet, but also with regard to their perception of the world and the risks that it entails. While teachers seem to talk about the internet as an application or tool which potentially distracts from real life, youth discuss their online environment as a world of its own. This gap in perspective seems to have implications on the types of risk that is perceived by each group. While teachers did recognize some basic risk, such as internet scams and the internet as a distraction from their student's studies, they did not indicate a strong awareness of what apps children were using or where they specifically experience risk online. While teachers have seemed to be aware of some limited risks (such as pornography and internet scams) through social media, children identified a much more nuanced field of risk, including gaming apps, which are used as a venue for meeting children, and detailed accounts on grooming on social media platforms, as well as live-streaming sexual exploitation.

Children and teachers propose similar solutions like user awareness, internet time management, library access, and the need for reporting and taking down contents. However, children demonstrate a much more nuanced view of risk and suggest more practical means of encouraging children to report OCSE-related content and work with social media platforms to provide a more adequate response to child-protection reporting. Further, solutions from teachers tend to focus on actions that need to be taken in the offline world, while children tend to focus on actions needed to be taken within their online environments. Teachers see solutions in increased law enforcement and preventing children from having access to the internet and cite the need for greater reporting and take down of abusive content, while children were more likely to cite the need for user awareness, reporting, monitoring, and collaborating with parents and teachers to keep children safe. Children seem to value the positive worldwide interactions that they have been afforded through their online environments, but also recognize the immediate need to mitigate risk for they and their peers through better online education, advocacy, and more responsive child-protection reporting and response mechanisms.

# Chapter 4: National and International OCSE Reporting Mechanisms

## 4.1 Governmental Specialist Department:

The Royal Government of Cambodia (RGC), established the national committee for anti-human trafficking (NCAT) is significant progressing to prevention, protection and respond to all forms of trafficking and exploitation. The committee members representation from inter-ministries and institutions, also all of provincial anti-human trafficking.

Meanwhile, MoI established and enforced for two specialist department under National Police Commissioners as department of anti-human trafficking and juvenile protection and the department of cybercrime played important roles for cooperation, intervention, and respond timely and in collaboration with INGO/LNGOs to solve the issues in related to OCSE. With this, the telecom regulator of MoPTC is one of mechanisms to manage the internet service companies in Cambodia and intervention with a technical mandatory after receiving the requested for any guidance, protection, and have authorities to terminate the website who have contents in relate to OCSE.

## 4.2 National Center for Missing and Exploited Children (NCMEC)

In the United States, all Electronic Service Providers (ESP) are required to refer any potential child protection cases to the Cyber Tipline, operated by the National Center for Missing and Exploited Children (NCMEC). This mandate includes all ISPs and technology companies based in the United States (Facebook, Microsoft, Google, Twitter) and foreign companies who use US-based servers to house their data. Because US technology companies provide a large portion of the infrastructure for the world's internet, NCMEC receives a great deal of global reporting on OCSE (in particular, CSAM) and serves as a clearinghouse for these reports, providing basic analysis, collation of key investigative information, and referral of reports to law enforcement around the world.

When a user reports child sexual abuse material on an online platform, such as Facebook, that material will be reviewed by the platform and removed/reported if it is found to be in violation of the platform's child-protection standards. If the image depicts child abuse or exploitation, the image, the user's account, and the IP address will be logged, along with other key information, and included in the reporting forwarded to NCMEC. The users IP address provides information about the geographic location where the potential CSAM originated, as well as what local ISP the materials passed through when it was uploaded from or downloaded to the potential perpetrator's ICT device.

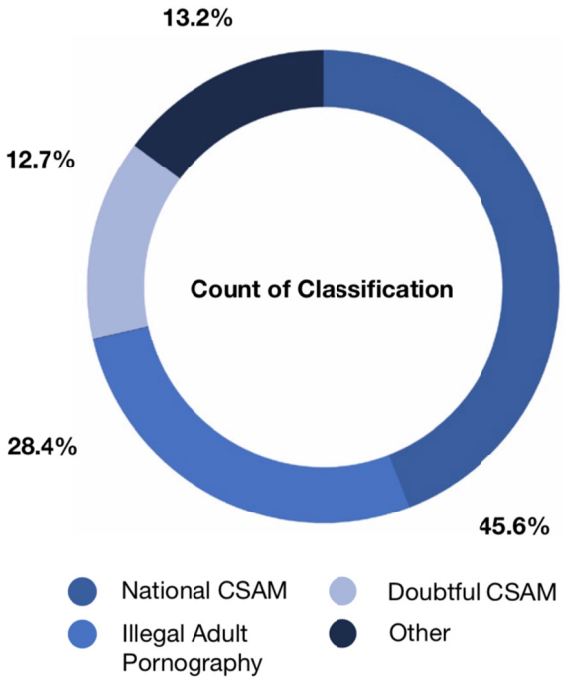
In Cambodia, any Cambodian-relevant CSAM reporting is automatically forwarded to United States Homeland Security Investigation (HSI) agents, located at the US Embassy in Phnom Penh. HSI agents in Phnom Penh are then responsible for downloading reports and determining what cases are most urgent and actionable at the local level. Over the past six years, there has been a steady increase in this reporting to HSI in Phnom Penh, especially for the year 2018. While complete numbers for 2018 are not yet available, CSAM reporting to Cambodia from January to November 20, 2018, indicates a 490% increase from 2017. Meaning that, within the first 11 months of 2018, NCMEC referred 123,896 CSAM reports to HSI in Phnom Penh, which is more than has been referred over the past six years, combined (see figure below).

| Year | VPN | Informational | Total |
|---|---|---|---|
| **2013** | 370 | N/A | 370 |
| **2014** | 4,759 | N/A | 4,759 |
| **2015** | 5,292 | 24,133 | 29,425 |
| **2016** | 9,221 | 21,083 | 30,304 |
| **2017** | 4,832 | 20,500 | 25,332 |
| **2018*** | 32,913 | 87,983 | 123,896 |

*2018 – though 11/20/18

Not all of the images sent to HSI may qualify as CSAM, but could include child nudity, various forms of violence against children, or other flagged images that are in violation of the service providers content standards. Thus, before potential CSAM is referred to Phnom Penh, images are sent for basic forensic analysis for triage and to be provided with a priority rating, which allows HSI agents to identify the most urgent and actionable reports first, which will ideally be investigated alongside of local (Cambodian) law enforcement officials. This process will be explained in the following sections.

NCMEC identifies two types of potential CSAM reports: Informational and VPN. An informational report refers to an image that has potentially gone 'viral' or has appeared on a series of social media accounts through shares. Informational reports usually provide additional "information" about the spread of a particular potential item of CSAM, or otherwise inappropriate item. Informational report are usually reports on an item which has potentially gone viral and might not represent a new, actionable instance of CSAM. On the other hand, VPN reports usually refer to something that seems to be new, hasn't necessarily been passed around on the internet, and is believed to be CSAM at that point. Reports such as these could potentially be actionable evidence for law enforcement if adequate surrounding evidence exists.



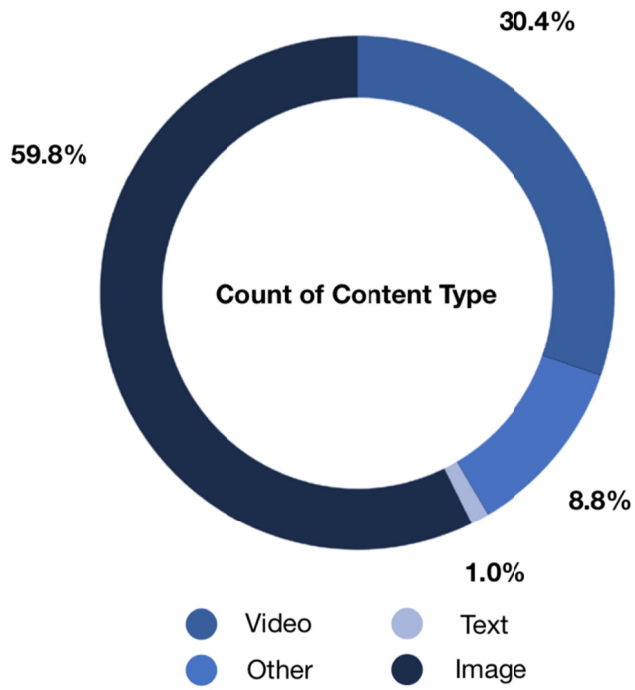

Over the past six years, only 43% of Cambodian CSAM reporting referred from NCMEC has been VPN reporting. However, VPN reporting has shown a significant increase in 2018. The 32,913 VPN reports referred to Cambodia from January to November 2018, is nearly 1.5 times greater

than all of the reporting referred to Cambodia in the five previous years, combined. This indicates a significant increase in new and actionable CSAM reports in Cambodia, which would demand greater resources, capacity, and practical support from local law enforcement throughout the country.

NCMEC indicates that this spike in reporting could potentially be due to a number of factors, including greater vigilance and proactive monitoring by social media sites, electronic service providers clearing reported CSAM off their servers, and/or an actual increase in the production of CSAM by users or offenders. NCMEC Representatives indicate that CSAM reporting from NCMEC is user specific, meaning that If a user has one CSAM image, NCMEC will send a report for one image. On the other hand, if a user has a cache of 25 images, one report will be sent to HSI in Cambodia bearing reference to all reporting images under the user's account.

# 4.3 APLE Internet Hotline Reports

Over the past three years, 204 OCSE-related cases have been reported in Cambodia to the APLE Internet Hotline, which is a part of the INHOPE Network. While user-generated reporting is often able to capture a more diverse spectrum of OCSE content, it often captures only a small portion of the cases visible on the open web. Internet Helpline cases rely solely on the vigilance of internet users throughout the internet, who are aware of the hotline and willing to submit a report on the child-protection concerns that they come across. The persons reporting these cases always remain anonymous, unless the user chooses to disclose their identity— which is very rare. Among the 204 cases reported to APLE Internet Hotline, 200 or 98% were reported anonymously.




Of the 204 cases, 93 or 45.6% are confirmed cases of child sexual abuse materials (CSAM) involving Cambodian children. In addition to these, 27 cases or 12.7% are unconfirmed CSAM or materials that appear to be sexually abusive content featuring children, but the age of the person in the content is unable to be confirmed. This is often due to content that is blurred, incomplete, or only features certain sections of the body. Further, nearly one-in-three of the 204 cases, or 28.4%, have been determined to be sexualy explicit content of persons over the age of 18. This can include materials recorded privately or live-streamed in a private session, which are then posted publicly— generally against the wishes of the person featured in the sexually explicit content. APLE Internet Hotline still responds to adult reports such as these by seeing that the content is removed to protect the victim whose private content has been publicly exposed.

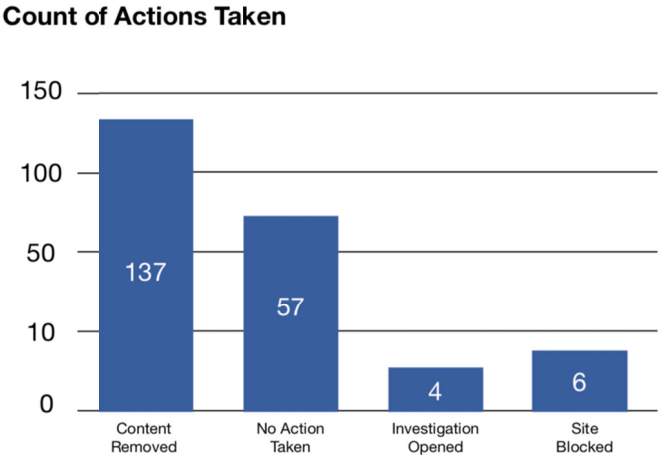
The majority of content reported to APLE Internet Hotline, 122 cases or 59.8%, are in the form of still images of child sexual abuse. Nearly a third of cases, 62 or 30.4%, are in the form of video files. A minority of cases, 18 or 8.8%, are classified as "other". This content can include a variety of harmful or abusive items including children being physically abused or instances in

which public/non-explicit photographs of children which may have been photoshopped or edited to appear as though the child was naked or in another form of explicit situation. Lastly, two cases reported were in the form of text messages.

Only 44 cases, or 21.6%, were able to be identified as child sexual abuse occurring in Cambodia, while in the majority of cases (77.9%), the location of the abuse was unable to be determined. Similarly, the ages and gender of the victims are unable to be determined in the majority of cases. Among the cases in which the gender of the victim is able to be determined, 32 or 68% are female, 6 or 12.7% are male, and 9 or 19.1% of cases involve both males and females. In 157 cases, a gender distinction is either missing or not able to be determined in the report. Among the 43 reports in which age was able to be categorized, 18 or 41.8% were categorized as "adolescent", 10 or 23.2% were prepubescent children, 4 or 9.3% were toddlers, and 1 or 2% was an infant. Lastly, 10 reports were categorized as persons over the age of 18— most of whom had been featured in sexually explicit content against their wishes. In 41 cases (20%), the ethnicity of the victim was able to be established. Among the 41, 34 or 82.9% were Asian, 12.1% were white, one was african and one seemed to be of mixed ethnic backgrounds. Nationality was only able to be determined in 20 cases, 19 of which were determined to be Khmer, and one who was determined to be Thai— the remaining values were either missing or unable to be determined.

The majority of cases, 125 or 61.3%, were referred to the internet host (which owns the servers on which the CSAM is stored) for removal. A host could be a well-known company such as Facebook or Youtube, or a lesser known website or social media platform where the original CSAM was found and reported. In the majority, or 110 of the 125 cases (88%) reported to the host or web domain, the CSAM was removed. A week after reporting CSAM for removal, an APLE Hotline analyst will review the case and assess that the material has been removed, however, in 15 of the 125 cases (12%) no action was taken on the part of the internet host. Further, in six cases (2.9%) full websites resulted in being blocked as a result of an APLE Internet hotline report.

Over the past three years, only 16 or 7.8% of cases reported through the APLE Internet Hotline have been referred to law enforcement and only 4 or 2% of cases have resulted in an investigation being opened. A case is only referred to the police if a victim is about to be identified and there is sufficient evidence available in the report to open a case. In most cases, the CSAM report is either determined to not require police follow up, or in cases where follow up is required, there is insufficient evidence to do so.




In 30 of the reported cases, or 14.7%, the CSAM content was determined referred to INHOPE network of internet hotlines. Cases are referred to the INHOPE network in situations where, the CSAM content is found to be hosted in another country that is an INHOPE partner, or the victim in the content is identified as being a national from a country that is an INHOPE partner.

The year 2015, which was the year the hotline was created, had the fewest number of CSAM reports to the hotline. The following year, 2016, CSAM reporting seemed to peak with 71 cases of CSAM reported to the hotline during this year. In subsequent years, reporting of CSAM seems to have reduced with 58 reports in 2017 and 43 reports as of the writing of this report. The decrease in reporting is likely due to a lack of user interaction with the hotline, rather than a

decrease in the occurrence of OCSE. In fact, according to reporting from NCMEC, CSAM reporting has shown a nearly 370% increase over the past year (2017-2018).

# 4.4 Child Helpline Cambodia

Despite the high volume of calls that the hotline receives each month, only seven OCSE-related cases have been reported to Child Helpline Cambodia within the past three years. The majority of cases (or five of the seven) involve instances in which sexually explicit pictures of a young person have either been posted to social media without their consent or images are threatened to be posted if the young person doesn't comply with the requests of the person holding the images. In one case, the person holding the sexual images of the victim demands payment in order for the sexual images to not be released and in another case, such images are held as a threat to keep the victim in a relationship with the offender. In one case, the victim and perpetrator had previously met for a sexual encounter and explicit images had been taken without the young person's consent— the victim cites fears that the images would emerge publicly on the internet. One case seems to involve potential grooming, where the victim cites an unknown person (which has been added as a friend on Facebook) began sending sexual images and wanted reciprocation from the victim. When the victim denied, threats were made to post images of the victim (which has been photoshopped to appear sexually explicit) publically to a social media site.

All young people reporting cases were Cambodian nationals and six of the seven were female. Because the Child Helpline Cambodia receives cases from people until the age of 25, three cases were from young people who were 18 and the remaining cases came from young people over the age of 18. In three cases, the victim was unable to be contacted for follow up actions so no actions were able to be taken. In two cases, the victim was provided with information on content blocking and referrals for service. Another two cases resulted in legal action, one locally in Cambodia and another in a foreign country where the perpetrator was located.

Regardless of the low incidence of reporting, similarities in content are notable between the cases of OCSE discussed in learning workshops and those reported to the helpline. These patterns will be addressed in later sections of this report.

# 4.5 Investigating OCSE Reports

Few OCSE investigations are ever initiated by an in-person report to police. The majority originate from law-enforcement referrals of CSAM images discovered on electronic devices belonging to child sex-offenders, collections uncovered on dark-web forums and on peer-to-peer file servers and CSAM reporting from organizations like NCMEC generated through child-protection reporting on internet platforms such as Facebook or Google. In order to discuss the investigative process of such OCSE-related cases in Cambodia, it is necessary to first explain how reports are generated and what resources are most commonly available to conduct an investigation.

## 5.5.1 Reporting from NCMEC

If there are particularly serious acts going on or if the report is a part of an active case, NCMEC reports will be independently sent to the FBI. However, the majority of NCMEC reports/leads go directly to HSI through an online portal. According to HSI field agents, most of the leads in Cambodia originate from Facebook and Google. Reports emerging from the portal are usually less than a week old when they are made to available to agents in Cambodia and include, images/video evidence, IP addresses involved and a basic rating of the seriousness of the CSAM involved in the case. Analysis of images is cursory, but basic image classifications are

provided in HSI reports, which are made available for local law enforcement. Classifications for image content are as follows:

> 'A' – Juvenil "not sanitary"
>
> 'B' – Juvenil "sanitary"
>
> '1' – Sex Act, any image/video of sexually explicit conduct
>
> '2' – Lascivious exhibition, any image/video depicting nudity and one or more of: restraint, sexually suggestive poses, inappropriate touching, etc. etc.

Combinations can be formed using the above classifications. For example, one image may be categorized as A1 or B2 or A2 or B1. Data coming through this HSI portal from NCMEC is quite advanced, including IP addresses and other identifying markers for the device tied to the distribution of the CSAM. HSI cites receiving between 700 and 1,000 reports through the portal in a month.

Once HSI receives the reporting, agents will break them down, usually start with the 'A' categories, which involve the more egregious crimes against children. The NCMEC lead would indicate that a particular IP address had downloaded or distributed a certain CSAM item. Agents would then need to track down the IP address. This is very difficult within the Cambodian context as ISPs do not have any particular set standard for maintaining IP assignment log data and, in many cases, the basic data needed to follow up on reports and open an investigation is no longer available by the time a request is made.

### 5.5.2 Interpol ICSE Database

The International Child Sexual Exploitation (ICSE) Database is an investigative tool owned and maintained by Interpol. The database is used by certified law enforcement officers to investigate CSAM in the form of images, videos, and hashes, and compare them to other data and evidence seized by law enforcement, worldwide, which is also stored in the database. The Interpol National Central Bureaus hold primary control over the access of their national users to the ICSE Database. The primary purpose of the database is to facilitate the identification of child victims of sexual abuse and reduce redundancies in identification efforts by law enforcement. To be connected to the ICSE Database, a country must have specific legislation proscribing CSAM/CSEM, a specialized national unit working with victim identification, and sufficient bandwidth to support the operation of their connection to the database At present, law enforcement and other key personnel from 54 connected countries, as well as INTERPOL and Europol officials are connected to the database and use it to share seized CSAM and other case-related information.[55]

When a user (generally a member of national law enforcement) uploads a new child-sexual abuse image, image hashes are used to search for existing images, and to verify whether new media already exists in the system. Image hashes function as a type of unique fingerprint for any digital images. Since any digital image is composed of particular attributes, such as pixels, colors, and dimensions. These attributes can be translated, by computers, into a unique digital code that precisely represents a particular image. This code is known as the image's "hash value". This text value can be used to search for exact copies of the same image throughout a database. Therefore, even if the same image was uploaded by a different country, tied to a different case, and under a different file name, the images hash value remains the same and can be used as a unique identifier and a means reducing duplicate images within the database.

While the ICSE database receives CSAM data from law enforcement officials in member countries, NCMEC often has wider access to potential CSAM as they continually and automatically receive reports from US ISPs and large tech companies (such as Facebook,

[55] ECPAT. (2017).

Google, and Microsoft), which are required to report all OCSE-related content to NCMEC under US law. Thus, there is a collaborative agreement between NCMEC CyberTipline and the Interpol, which allows Interpol to have access to the hash values of the images collected by NCMEC. In cases where a US police unit is not directly in charge of a CSAM case (such as a CSAM image of a Cambodian child uploaded to Facebook by a Chinese person in Cambodia), NCMEC has the capacity to upload the CSAM image and relevant case information directly to the ICSE database. This allows international law enforcement to pursue active child protection issues, which would otherwise be outside of US legal jurisdiction.

The ICSE Database is a victim-centered tool, which aims to support law enforcement in identifying child-victims. Thus, media in the database are categorized as either *identified* or *unidentified.* Identified children are labeled as such so as to minimize the likelihood of any duplication of effort relating to the identification of those victims and unidentified children are labeled with the aim of identifying the children. The ICSE Database, and its ability to effectively identify children, relies on the case owners at the local level to update the status of cases, to enter case information, and to utilize local-level knowledge and evidence to identify images of Cambodian children appearing in the database.

The voluntary nature of database administration means that the amount and quality of information it contains is contingent on the will and resources of these individual users. At present, the Cambodian National Central Bureau (Interpol attached office in Cambodia) does not have direct access to the ICSE database. Because of this lack of collaboration, there are difficulties in utilizing the ICSE database to its fullest potential in Cambodia. Without a national-level connection between Cambodian law enforcement and the database, international law enforcement face difficulties in understanding themes and patterns of OCSE offending in Cambodia in that the information within the ICSE database relies heavily on national police and their capacity to utilize it and contribute to it.

There is a distinct need for greater cooperation and input from ASEAN and East Asian nations into the ICSE Database. International law enforcement is aware of child sexual abuse/exploitation materials produced in Cambodia by travelling offenders from Korea, China, Japan, and other nations, however, they are unable to identify children and investigate offenders without active participation and collaboration from regional and local partners. At present, western nations (Europe, UK, US, Australia) have made great progress in addressing the issue of their nationals traveling to ASEAN region for child sexual abuse and exploitation. However, police attaches from ASEAN and East Asian nations (including Korea, China, and Japan) often do not put forward child-protection as a priority. International Law Enforcement officials describe a particular increase of Chinese nationals involved in the production of CSAM, but when these cases are referred to Chinese police attaches, there is often limited-to-no further communication on actions taken or the outcomes of the cases.

Social norms do not always condemn sexual offenses against children in some East Asian nations. In many areas, Children can be sexualized with few social repercussions. Law enforcement in these areas is not proactive on OCSE-related cases and international collaboration is minimal, with a greater focus placed on responding to fraud, money laundering, and other financial related crimes. This creates a unique challenge for understanding and dealing with Asian and ASEAN child sex offenders throughout the region..

Further, there is a need to unify the process of dealing with CSAM to ensure that all images are hashed, indexed, and access is given to international law enforcement. At present, when CSAM discovered by police in the country is not being passed on to Interpol and processes and standards for dealing with caches of CSAM need unified between international and local law enforcement agencies. This requires the establishment of a secure connection between Phnom Penh NCB office and Interpol to facilitate this process.

There is also a significant need for persons in criminal justice to be able to understand and utilize the sites on the dark the live-streaming facilitator connects perpetrators with victims. At

present, law enforcement is currently reactive to crime, but there is a need to become more proactive in investigating potential child-protection issues. While lawmakers and members of the judiciary have strong voices in the development of legislation and policy for the prosecution of OCSE-related crimes, international law enforcement cites that these entities are not frontline observers of the issue in the way that police and child-protection specialists are. Thus it is important for frontline practitioners to be allowed to have a more active role in the development of policy to support their ongoing work.

### 5.5.3 About ISPs and IP Addresses

ICT devices such as smartphones, computers, tablets, etc, cannot connect to the internet directly. They must first connect to a local network or router (such as a Wifi network or a cellular tower, if the device is using mobile internet) and then that network connects to an Internet Service Provider (ISP). The ISP is directly connected to the internet and serves as a gateway for the device (and local network) to have access to the internet. At any point in time, there may be hundreds or thousands of devices connected to a local network and hundreds of thousands connected to an ISP. In order to ensure that the information on the internet is delivered to the correct device, on the correct network, in the correct city, within the correct country, ISPs will assign each device a unique address to keep things in order. This is called an *IP address*.

An IP address is a unique series of numbers which are assigned to a device (like a smartphone or computer). It is usually represented as a set of four numbers separated by dots (“.”), such as 192.168.0.100. This address is automatically assigned to a device by the ISP in order to identify the device so that information can be correctly sent from the device, through the ISP, to the internet, and back to the device. Therefore everything that a user does on the internet is automatically linked to, and identifiable by, this address.

Most networks and ISPs use “dynamic” IP addresses. This means that a new address is assigned to every device, each time that it is turned on and connects to the internet. Because IP addresses are always changing, detailed records are needed to know what IP address was assigned to a particular device at a particular time. These records are called *“IP Assignment Logs”*. For example, if someone sends a message from a laptop computer through Facebook at 8:30 am, the ISP may assign the laptop the address 0.0.0.1. If that person, closes the laptop and then reconnects later at 11:30 am, the ISP may assign the address 0.0.0.2 and the previous number (0.0.0.1) may be assigned to a different laptop, which is accessing the internet at 11:30 am. An *IP assignment log* would keep track of the location of each IP address at any given time, what computer it was assigned to, and other relevant information about the specific device and internet session.

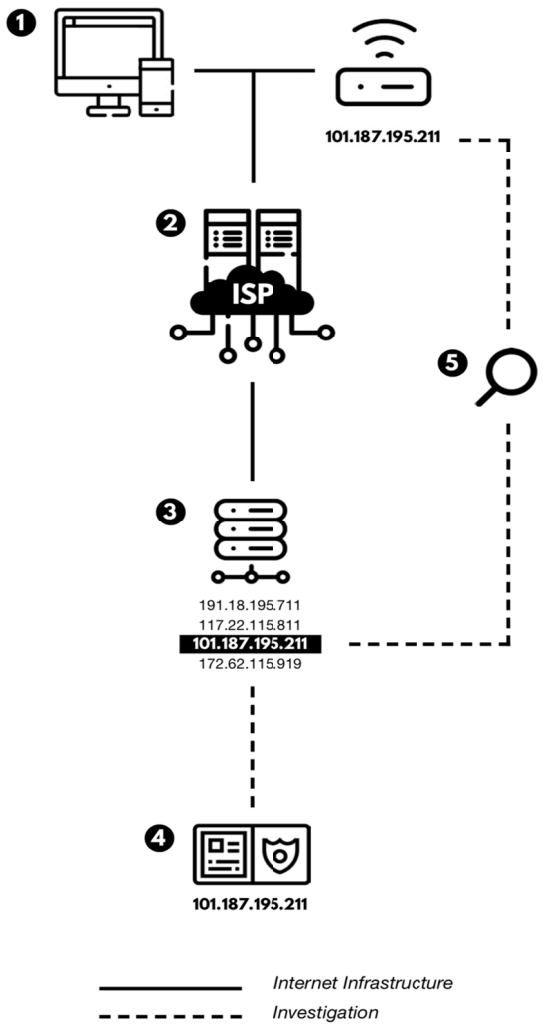
When a child-protection or law enforcement agency, like NCMEC, Interpol, or APLE identifies a new case of CSAM being circulated, the report usually consists of an IP address and basic information about the child abuse materials that were sent or received through that IP address. In order to know the physical location where this material came from, and potentially, the person distributing it, the agency would need to have access to the “IP Assignment Logs”, which are in the possession of the ISP. In the United States, all ISPs are required to save these logs for a minimum of 6-months, so that law enforcement can investigate in the case that a crime has been committed on the internet. In Cambodia, there is no standard for saving IP Assignment Logs. Some ISPs may save logs for a matter of weeks, others for a matter of days, and others for only a matter of hours—making investigation of the incident virtually impossible.

Cambodia-based members of United States Department of Homeland Security indicate that this is a significant issue, which prevents Cambodian law enforcement from investigating the leads provided to them through NCMEC. Because OCSE is typically identified using IP addresses, it is not possible to know where the crime (of distributing CSAM) was committed without access to these logs, which allow law enforcement to identify the location of the device that is producing or distributing CSAM or otherwise causing harm to children. This does not refer to the

production of CSAM, which often requires a greater forensic analysis of the CSAM images or videos themselves.

# How Do IP Address Assignment Logs Work?

A simplified explanation of the tools ISPs use to identify internet users and how this could be useful to investigators responding to an online child-protection issue.




## INTERNET INFRASTRUCTURE

1. ICT devices (such as smartphones, computers, or tablets) cannot connect to the internet directly. They must first connect to a local network or router, which then connects to an internet service provider or ISP.

2. ISPs are the gateway to the internet. They could be a mobile phone company, which provides mobile internet (like 4G or LTE) or the provider for a fixed internet connection from a home or office. An ISP may have thousands of devices connected at any given time. So, in order to deliver information to the correct device in the correct place, ISPs assign each connected device a unique series of numbers for identification. This is called an IP address.

3. Since a new IP address is assigned each time a device connects to the ISP, a single device may have many IP addresses over a given period of time. Thus, detailed records must be kept in order to know what IP address was assigned to a particular device at a particular time. These records are called "IP assignment logs".

## INVESTIGATION

4. If law enforcement learns of a crime that has been committed on the internet, such as the creation or distribution of Child Sexual Abuse Material (CSAM), the police report may contain the IP Address that the CSAM passed-though on it's way from the device to the internet.

5. With sufficient criminal evidence, law enforcement can request to see the ISP's IP assignment logs, which can show what local network (and potentially, device) the IP address was assigned to at the time the crime happened. This can be an important way for law enforcement to find offenders and protect children. Thus, maintaining IP assignment logs can be an important part of responding to child-protection concerns on the internet.

# 4.6 Challenges to Investigation

While the monitoring made available through NCMEC and other child-protection agencies is helpful, these resources depend on the ability to trace IP Addresses to a particular name and geographical location, in order for the crime to be investigated. While improvements in the nation's registration and logging of IP addresses would greatly help to provide better protection for children throughout the country, there are still numerous other vulnerabilities currently being exploited, which keeps perpetrators safe and children at risk. These include the law enforcement of SIM card registration, peer-to-peer (P2P) networks, and the 'dark web' for anonymity.

## 4.6.1 Unregistered SIM Cards

Many mobile phone SIM cards in Cambodia are unregistered, thus the IP addresses associated with these Smartphones are not able to be associated with the phone's owner, which makes investigation of crimes associated with that phone's internet connection difficult. Previously, all mobile telecom providers required to provide identification when customers purchased a new SIM card. Despite the legal requirement for all telecom companies to request users register new SIM cards with identification, this regulation is commonly not enforced. Further, as more telecom providers began entering the market and competition increased, some new companies began distributing free SIM cards— many of which were never registered, allowing users to remain anonymous.

In 2015, the Ministry of Post Telecom and the Cambodia National Police Commissioners issued the first deadline for mobile service providers to register all their users. The deadline has been extended multiple times since then, following requests from Cambodia's three largest mobile operators (Viettel, Cellcard and Smart Axiata) to be given more time to comply with the requirement. The final deadline for registration, nationwide, was extended to July 1, 2018. Following this date, all telecommunications companies in Cambodia were required to ensure all their SIM card users were registered.[56]

National telecom regulators indicate mobile operators have largely shown good commitment to complying with the new regulations, however, loopholes usually arise with local dealers who will sell SIM cards on behalf of the mobile operator. While the operator will require that all dealers provide customer registration information, dealers are often cited tol input incorrect or fraudulent registration information as a way of cutting corners. Despite this, national internet regulators estimate that less than 10% of current SIM cards remain unregistered, but indicates determination to continue the enforcement of registration throughout the country.

## 4.6.2 The Dark Web

The Dark Web is a part of the World Wide Web whose contents are not indexed by regular internet browsers, such as Chrome or Firefox. The Dark Web consists of websites that are visible to the public only through the use of a special internet browser (such as ToR or Freenet), which relies on a network of anonymous, interconnected computers around the world to host its contents. The Dark Web's network intentionally hides user IP addresses and since IP addresses are used to determine the user's location, and the servers being used to host the websites, and content being accessed[57], users are able to remain virtually invisible to anyone else on the network, including governments and law enforcement. The opposite of the Dark Web is the Surface Web, which is readily available to the general public and searchable with standard web search engines, such as Google.

[56] Chan, S. "Government issues deadline to register sim card users", accessed 15 Oct, 2018 from, https://www.khmertimeskh.com/50505669/government-issues-final-deadline-to-register-sim-card-users/
[57] Technopedia. (n.d.).

The Dark Web is commonly used by journalists, researchers, and human rights advocates to keep them anonymous and protected while developing intelligence and in risky world areas. However, it has also been co-opted in recent years by persons wanting to use it for more illicit activities, including human trafficking and the sale of drugs, weapons, and other illicit products and services. Pedophiles commonly use the Dark Web as a resource to anonymously connect with one another, build social and resource networks, and share CSAM/CSEM. NCMEC cites receiving a number of public reports on instances of CSAM/CSEM on the dark web. These are very limited, however, as this relies on the public taking the initiative to report since this is not something that is commonly picked up by electronic service providers.

### 4.6.3 Peer-to-Peer Networks (P2P)

Peer-to-peer (P2P) networks are the most popular mechanism for the acquisition and distribution of CSAM/CSEM.[58] These networks provide a way for users to directly share files between two or more people without having to store the files on a central server.[59] This allows users to transfer files from one IP address to another directly without revealing the identity of their network or the device that they are using. Research into CSAM/CSEM on P2P networks have demonstrated a large amount of traffic on these network that is dedicated to such materials. However, while CSAM/CSEM represents a large amount of traffic, it is not believed to be a majority of the traffic on these networks, as only 1% of queries are found to be related to such materials, which is consistent with similar research into the same area[60]. More research and child protection work needs to be done to address the acquisition and distribution of CSAM/CSEM within these contexts.

[58] Hurley, R., et al. (2013).
[59] Netclean. (2017).
[60] Steel, C. M. S. (2009).

# Chapter 5: Cambodian Capacities and Challenges

## 5.1 Criminal Justice

The lack of data reported OCSE-related case from the local law enforcement is cited to have been a significant challenge over the past 10 years. This has been especially true within Asia—as most countries do not have reliable national reporting mechanisms integrated with national law enforcement. It is important for national mechanisms to actively address the issue of OCSE on multiple fronts, including partnering with the financial sector, creating awareness around the various payment systems used to compensate producers of CSAM, including services such as Western Union, Wing, Cryptocurrency, and other anonymous forms of sending money. Systems such as these have become well established throughout the SE Asia region.

### 5.1.1 National Law Enforcement Awareness and Capacity

Cambodia has established an Information and Technology Office under the Anti Human Trafficking and Juvenile Protection (AHTJP) Department and an Anti Cybercrime Unit under Cambodia National Police Commissioner. MoI established unit of cybercrime operation is under the Criminal Investigation Department. While both offices are technically comprised of judicial police officers and have the mandates over OCSE, neither of these offices have established specific priorities, responsibilities, or practical mechanisms for responding to OCSE. In practice, the Cybercrime unit generally carries the responsibility for computer-related crimes and AHTJP would deal with crimes related to child trafficking and exploitation. Thus, child exploitation cases usually will begin with AHTJP and, if the child exploitation case involves technology, the case would then be referred to the Cybercrime unit for evidence examination and investigation.

While the Cybercrime Unit has become the de-facto unit to carry the responsibility for providing follow up and investigation on OCSE-related crimes, the unit is a small team of about 10 people with limited resources and a large mandate covering a broad-range of computer-related crimes including: identity theft, hacking, and money laundering. Because of this broad mandate, international child protection advocates indicate the team lacks the bandwidth to address online child protection concerns.

#### 5.1.1.1 Anti Human Trafficking and Juvenile Protection (AHTJP) Police

##### Experiences and Awareness of Online Child Sexual Exploitation

The awareness of OCSE among National police (which includes AHTJP) seems to be limited to physical contact between an adult and child in an offline environment. Leadership within national police do not indicate a strong awareness of OCSE in general or the breadth of the internet's role as a venue for child sexual exploitation within Cambodian communities. The majority of awareness seems to center around traditional cases of child sexual abuse and exploitation, in which a perpetrator uses an online platform (especially Facebook) to arrange to meet a child for offline abuse. This awareness seems to be built around existing and previous cases directly reported within their division—which overwhelmingly involve traditional cases of child sexual exploitation. Officers did not indicate a significant awareness of online abuse in which the perpetrator is located in another country.

Police indicate a particular awareness of victimization of children from low income communities and an overarching assumption among law enforcement that OCSE is a foreign-perpetrated issue. One high-level official from National Police indicates that the only OCSE-related cases that he has seen have involved foreign perpetrators and cites that he has no information on the issue with regard to Cambodian perpetrators. This is possibly due to the fact that many OCSE cases with an identified perpetrator are referred through Interpol— whose focus is transnational crimes, which are often foreign perpetrated.

In the Siem Reap area, a key AHTJP officer observes that most children involved in OCSE (specifically CSAM) are children from the street, indicating that perpetrators will offer them financial support and, in some cases, raise them. Law enforcement indicates youth that will see pornography online and want to imitate what they see. One officer indicates a growing number of cases in which community members report students who become sexually involved with perpetrators in exchange for various forms of financial support. Many of this cases indicate a degree of networking among youth who are cited to rent rooms and live together, separate from their parents. Officers seem to associate victims in this context with disobedient children, describing them as drug users, school drop-outs, and 'teenagers who do not like to stay with their families'.

While officers indicate little knowledge of how the internet might mediate sexual exploitation, it is likely, given the climate described by children within learning workshops in this area, that the internet (particularly smartphone apps) could play a key role in the facilitation of cases such as these. Research on OCSE within a similar context in the Philippines[61] found a similar phenomenon of children who become a part of a type of 'surrogate family' or 'gang', which provides money, social identity, and a level of protection in exchange for their participation in live-streaming OCSE. Social workers in the Philippines indicate a somewhat high-level of organization in these cases. It's unclear if there are any potential similarities in this context, however more research is needed.

In some instances, law enforcement indicate awareness of potential OCSE cases based upon evidence gathered from electronic devices confiscated during the investigation of a traditional child sexual exploitation case. In cases such as these, electronic devices belonging to the perpetrator are confiscated and searched by the CyberCrime unit (discussed below) and CSAM materials are discovered. APLE leadership indicates CSAM is discovered in about 60% of cases where child sex offenders are investigated. However, when a cache of CSAM is uncovered, police are only interested in a small sample of the images for prosecutors to prove the molestation charge. Officers do not commonly consider the full cache of CSAM as evidence of other crimes committed against children, or share such evidence with international law enforcement bodies, such as Interpol and its ICSE Database.

Officers cite that only a few OCSE-related cases have ever been referred to police and nearly all of them have been for online grooming, for exploitation in an offline context. The majority of child sexual exploitation cases are reported by victims, teachers, and neighbors who see evidence of a crime being committed and go to the police. One key officer recounts the case of an adult who was reported to be showing children sexually suggestive games and other sexual content online. This person was reported by people within the community who noticed children who were physically with the perpetrator in an offline environment. Another issue within this context is that many people within Cambodian communities do not use the justice system in situations in which a sexual offense has been committed. Rather, people tend to negotiate sexual offenses privately. A 2018 report by Action Pour Les Enfants (APLE) describes this issue and local authorities having knowledge of online grooming and sextortion case that has happened through Facebook, but not being able to proceed with investigation because the family involved were unwilling for the case to be reported and negotiated with the police to have the case closed.[62]

Overwhelmingly, the awareness of children at risk among national police (and adults, broadly) seems to be limited to the physical (offline) world, and does not indicate the possibility for children to experience sexual abuse or exploitation solely within an online environment. This seems to overlook the internet's role as a potential venue for child sexual exploitation and broadly ignores other potential forms of OCSE, including, grooming for the production and distribution of CSAM online, live-streaming sexual exploitation, and sextortion cases, which are all commonly indicated within learning workshops. Due to these assumptions, it would be

[61] Terre des Hommes-Netherlands. (2018).
[62] Action Pour Les Enfants. (2018).

seemingly unlikely that child-protection concerns in an online environment would be perceived or reported when they occur.

Overall, discussions with youth and law enforcement officials indicate a notable disconnect between adults and internet-using youth. One high-level law enforcement official indicates the distinct need for younger, more tech-savvy Cambodians to join the national police. At present, the extent of child-protection investigations among national police are almost solely focused on the actions of perpetrators in the physical environment, as opposed to the digital.

#### 5.1.1.2 The CyberCrime Unit

The CyberCrime unit is a new addition of Cambodia National Police Commissioners of Ministry of the Interior (MoI), first starting work in 2016. The core task of the unit is to cooperate with other government agencies in conducting forensic investigations of electronic devices. The unit commonly receives requests from the anti-human trafficking department to search seized electronic equipment for documents, images, or other files to be used in the prosecution of a case. While the CyberCrime unit bears the responsibility for the investigation of all OCSE-related crimes, the unit is also responsible for any other computer or technology-related crime, including, attacks on computer systems, email spam, phishing, identity theft, online scams, and fraud. While the CyberCrime unit should ideally serve as a centralized hub for computer-related crimes, the division does not, itself, have the capacity to investigate crimes that were committed on the internet. At present, the bulk of their work and training focuses on the physical, forensic investigation of evidence held on electronic devices gathered from criminal raids, as opposed to crimes committed on the internet.

While the office and mandate exist, law enforcement in Cambodia do not presently have the capability to conduct investigations on the internet and present efforts of computer forensics are under-resourced. The CyberCrime unit has very limited experience with investigating any OCSE-related crimes. As a relatively new unit, they have (as of the writing of this report) investigated only 03 criminal cases involving electronic devices in their history, only 16 of which have involved children. Key officials cite that the office presently receive one or two computer-related cases per month, however very few of these relate to child-protection and fewer would fall under the category of OCSE. In part, the lack of case work on OCSE could be due to the fact that the work of the CyberCrime Unit is largely reactive, and often depends upon a case of OCSE being reported to the AHTJP, and then being referred to the CyberCrime unit. At present, there does not seem to be any proactive effort to deal with Online Sexual Exploitation of Children as a national issue, rather the unit acts based upon specific referrals from other government agencies.

Historically, much of the unit's "online" investigations concentrate on Facebook pages that are derogatory of Cambodian public figures or that are believed to be selling illegal items such as drugs or sexual paraphernalia. The extent of online investigations are extremely limited and are described to entail a review of the social media account in question for public phone numbers, email or physical addresses, and them following up with the account holder to have them remove the supposed illegal content. With regard to the "online" investigation of CSAM cases, key informants indicate that the majority have been on Facebook. Officers indicate that they simply refer cases such as these to Facebook's public content reporting mechanism through a link provided by Facebook, as the team has found this to be faster and more effective. A member of the team will send a request to Facebook and a reference (usually a link) to the CSAM image in question. If the child-protection case involves a particular Webpage, the CyberCrime unit would then refer the IP address of the Website to the private ISP to provide information on the end-user in question. However, this is often impossible due to the fact that most ISPs to not consistently maintain their IP assignment logs— an issue which will be covered later in this report.

Further complicating the identification of CSAM is the issue of social and cultural norms that do not necessarily problematize (much less criminalize) the posting of nude images of children in

public forums, such as Facebook. Even with pornographic images, the sharing pornographic images of people under the age of 18 is not always condemned and is understood as a blurred line by many throughout the country. This creates a a barrier to addressing the issue of OCSE in that it potentially decreases the likelihood that people in communities will report when they find images of a child in danger.

**Key Barriers to protecting children from OCSE**

Given evidence from communities and in-depth discussions with local and international law enforcement officials, there seem to be a number of significant barriers to the identification, investigation, and prosecution of OCSE-related crimes in Cambodia.

1. **Lack of knowledge of ICT Devices and technological trends**: National police cite that officers lack knowledge of current information and communication technologies and technological trends among youth. Despite having an information section in their office, officers cite that working with child exploitation in an online environment presents serious difficulties and is often filled with significant gaps. One officer notes that many young people are more advanced than most of the officers working to respond to internet-related crimes. Thus, without having knowledge of the online environments of youth or the methods commonly used by perpetrators to target youth, responding to potential online threats and investigating OCSE-related cases at a local level is nearly impossible.
2. **Lack of resources in local communities:** Due to the lack of technological awareness at the local level, nearly all computer-related crimes must be referred to the cybercrime unit in Phnom Penh. This requires officers to record any relevant information from the local level and submit it to the cybercrime division, which often involves bringing a physical device to the Cybercrime unit. This causes delays in investigation time and gaps in case information.
3. **Lack of collaboration with technical experts and international resources**: When a cache of CSAM is discovered (usually during the investigation of traditional child sexual abuse/exploitation cases) officers typically only preserve a small sample of images for the purpose of convincing a judge of a child molestation charge. The remaining images in the cache are destroyed and thus not shared with international child identification efforts through the ICSE Database. There is a particular need for this unit to be better connected to the Interpol ICSE database, which could not only give them the ability to identify children featured in CSAM discovered in caches taken from child sex offenders, but also allow for multilateral collaboration and capacity-building. Leadership within national police indicate a need for technical experts to support monitoring and investigation of these types of crimes so they can cooperate with experts and share information.
4. **Over-reliance on traditional, physical methods of investigation**: National police seem to place an almost exclusive focus on traditional criminal investigation, which often assumes a crimes that is physically committed by a perpetrator physically present within a community. In cases of OCSE, perpetrators may not be present within the city or even country, thus requiring law enforcement to rely on methods of online investigation and greater collaboration with international law enforcement, which can provide needed resources to investigate and prosecute crimes against Cambodian children committed by perpetrators located outside of the country. In some interviews, crimes committed in an offline environment were referred to as “real cases”—further emphasizing the need for crimes committed in an online environment to be recognized as “real”.

   According to a key representative from Cambodian Anti-trafficking police, law enforcement training on OCSE has been made available to Cambodian police, supported by the US embassy in Bangkok, however participants did not greatly understand the relevance of learning about new technology and methods of law enforcement, thus attendance (and information retention) is said to have been minimal.

Further, the use of complex and unfamiliar terminology, is said to have made the training difficult for officers to follow. This may emphasize the need for more contextualized and learner-centered trainings for current officers, as well as the need for the recruitment of more technology-savvy officers in the future.

5. **Lack of a victim-centered approach:** A victim centered approach seeks to place an equal value on the identification and care of victims as it does on the investigation and prosecution of offenders. While AHTJP officers may be aware of using a victim-centered approach in responding to victims of trafficking, national law enforcement seems to offer a more offender-centered approach in responding to and investigating internet-related crimes against children. In responding to OCSE and other potential internet related crimes against children, law enforcement seems to place a greater focus on identifying and prosecuting offenders (who may commonly be located outside of the country), instead of the identification and care of victims. In some instances, national law enforcement seemed to relegate responsibility for OCSE to police within the country where the perpetrator lived, rather than locally, where the Cambodian victim was located. This seems to further stress the need for greater collaboration and support from regional and international to not only share resources for the investigation of cases and prosecution of perpetrators, but also for support in practical training and capacity building.

As crimes move more and more out of communities and into online environments, vulnerable children within these contexts may become more and more invisible. Further, as computing relies more and more on information that is kept in the cloud or steamed live, physical hard disks and electronic means of data storage, will begin leaving virtually no prosecutable trace of a crime committed. Thus, it is important for the development of greater skill in enforcing Cambodian laws within these online environments.

# 5.2 Internet Service Providers

The Telecommunication Regulator of Cambodia (TRC) is the legal regulatory body that governs telecommunications systems. TRC oversees the maintenance of Cambodian internet infrastructure and the regulation and control of internet access across the nation. While TRC is technically in charge of internet control and access, it cites that the monitoring of inappropriate content on the internet is something that is usually undertaken by the Ministry of Culture and Fine Arts (MCFA), although the board has worked with MCFA in the past to address content issues.

The Internet Regulation board operates a hotline and Facebook page which serves as the national contact point for the public to report inappropriate content, hate speech, scamming, or grooming through the internet or other telecommunications devices. While the mandate of the regulator includes responding to public reports, a significant portion of the regulator's work seems to focus on responding to hate speech and derogatory remarks, especially against high profile figures within the country.

The board cites significant challenges in removal or take down of specific content because much of the content that is viewed in Cambodia could posted outside of the country and then stored on a server located in a separate country. Thus, tracking down the source and location of the specific content is a long and time-consuming process, which is cited to be beyond the capacity of the Internet Regulation Board to address.

TRC is able to ask operators (ISPs) to block specific content on the internet, in response to an official request from the government. Although, because most websites targeted for blocking are not hosted in Cambodia, TRC cites that it would need to issue an order to simply block the gateway to the website, through the ISP. This means that the site is only blocked for people

accessing the site through Cambodia. If TRC wants to fully take down the website, they would need to file a petition with the international organization that provides domain or hosting service to the website in question. If specific online content exists that the board wants to remove, which could be against Facebook's user policy, then the board is often able to process the take-down request through Facebook's public reporting mechanism. This is also the process taken by the CyberCrime Unit, under the Ministry of Interior, when responding to alleged inappropriate content on Facebook.

Further, a representative from the Ministry of Posts and Telecommunications (MPTC) describes a similar capacity for response against individual users who have been identified as abusive. MPTC indicates that, if they receive a complaint from a victim of abuse, they are able to investigate the incident. Upon identifying the user's IP Address, they will be able to know where the person is located and respond physically, or block the IP address. Although, given that IP addresses change regularly, and user's can easily use a VPN to disguise their real address, this level of response often not greatly effective. MPTC cites the need for greater education for people in communities to protect children from OCSE at the local level.

TRC states that it is unable to address child sexual exploitation on the internet. The board cites that even with a large team dedicated to monitoring the issue, it will not be successful because the majority of the sexually exploitative content is hosted on platforms, such as Facebook, which have their servers located in other countries. The Internet Regulation Board would not be able to respond to specific reports without blocking access to specific content on a platform without blocking access to the platform as a whole. The board believes that it is more important for the issue of OCSE to be address through children in communities, citing that children and their families do not understand the implications of sharing private or explicit content of themselves on the internet. TRC cites a greater need for awareness-raising in communities and teaching users to identify risks.

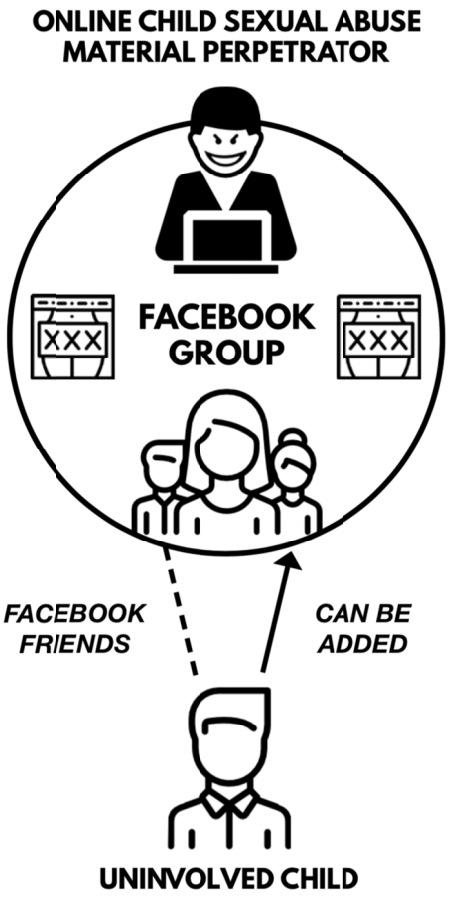
Within a rapidly-changing landscape of new technology, TRC indicates significant challenges in understanding the focus and reach of their agency's work. Previously, the regulator oversaw telephone communication in a nation having only one or two telecommunications (telephone) companies. Presently, within the new landscape of internet technologies, their work involves a long and diverse list of stakeholders including local internet service providers, local and international websites and web-platforms, as well as local and international content creators. The regulator cites that they, and other related government agencies, have struggled to define responsibilities for regulation of both services, users, and content. For example, many web platforms also process financial transactions and issue mobile forms of money, which should potentially involve regulatory oversight from the ministry of finance. TRC cites that government agencies are no longer able to work in separate silos, and describes the immediate need for greater collaboration between government agencies, as well as definition and delegation of tasks within the rapidly-changing landscape of internet technologies.

# Chapter 6: Discussion: What We've Learned

## 6.1 What we know about the NATURE of OCSE in Cambodia

Discussions with children and their teachers throughout the 16 learning workshops in Phnom Penh, Siem Reap, and Sihanoukville demonstrate a clear picture of the nature of OCSE-related risk at the community-level. Overall, the awareness of OCSE-related risk is notably high and includes an awareness of risks such as the solicitation and distribution of CSAM (27%), an awareness of various forms of live-streaming sexual exploitation (24.1%), the use of the internet as a platform for the grooming of children for sexual exploitation in both online and offline environments (28%), the distribution of adult pornographic materials and CSAM from adults to children (60.3%), and various forms of extortion on the internet using embarrassing or sexually explicit photos involving children (26%). Online surveys gathered from High School youth similarly reflect these findings.

Facebook and its Messaging app, Messenger, are the two platforms where the vast majority of OCSE-related risk and experiences are described as taking place. In many instances, the interconnectivity between these two apps seems to potentially place children at greater risk. While unknown Facebook users are not able to send unsolicited messages to children though the messenger app, they are able to search for the profiles of children on the Facebook app and send a friend request and the child is then provided with the option to respond to the user with a message. If the child responds in any way, the user is automatically given the ability to send messages, photos, and videos to the child, as well as the ability to initiate audio and video calls with the child. In many cases, the app will automatically suggest the friends of other children who may have already been added by the unknown user. Because the child sees friends in common, this can increase the likelihood that the child will respond to the friend request from the unknown user by either accepting the request or sending a message in response, which in turn gives the unknown user access to the child.




Receiving unsolicited pornographic materials (and in some cases, CSAM) from adults is the most commonly described risk on both Facebook and Facebook Messenger among Cambodian children. A key risk within this environment is the usage of Facebook groups. Within learning workshops, children described being added, without their consent, to Facebook groups which sexually explicit materials were shared. While unknown adults are not able to add a child to Facebook groups without first 'friending' the child on Facebook. However, if any of the child's Facebook friends have been added to the group, those children are then able to add any of their Facebook friends, without the Friend's consent. This allows children to be brought into sexually explicit or even exploitative groups without their consent.

While there seems to be a great deal of crossover with regard to risk on Facebook and its Messaging app, unique functions of each platform, which lead to increased risk to OCSE. While

Children recognize both apps as platforms where adult pornography and CSAM are sent and received, Facebook seems to be more of a point of contact for perpetrators to connect with children, while Messenger (as well as other messaging apps) are used as a platform for grooming and connecting privately with children. More than one-in-four children who describe Messenger as a risky app, understand it as a platform where strangers will attempt to build relationships with children in order to exchange sexually-explicit images or for other illicit activities. In addition to Facebook, Gaming platforms such as 'Rules of Survival' are also described as a platforms were potential perpetrators can make contact with children in a public, virtual environment to build rapport, get the child's contact information in order to make private contact on other communications platforms such as Messenger or Line.

While Facebook and its Messaging app figure greatly into children's environment of risk, OCSE in Cambodia does not seem isolated to a single platform or app, rather it seems to happen commonly over multiple interconnected apps and platforms. For instance, a child may meet an anonymous person within the context of a game or within a private group on a social media platform, and then, after adding the person as a friend (or sometimes just by sharing a sufficient amount of information, the perpetrator is then about to find the child and add him or her to groups or send private messages with the intent of OCSE or related harmful activities. Gaming and social media platforms seem to serve as an open environment for adults perpetrators and children with harmful sexual behavior to meet other children and add them on Facebook (which then allow private messaging through the Messenger app) or another private messaging platform such as Line or Skype where grooming or other OCSE-related activities might take place.

Children in this study do not describe specific instances of systematic sexual exploitation and violence as has been found in the Philippines[63]. However, there are still notable and widespread vulnerabilities to OCSE throughout all areas and among all groups of children in this project— particularly with regard to grooming and the production and distribution of Child Sexual Abuse Materials online. More research and further inquiry on the themes and patterns uncovered in this study should be conducted in order to better understand the experiences and vulnerabilities of Cambodian children on the internet.

# 6.2 What we know about the EXTENT of OCSE in Cambodia

It is not possible to generate clear statistical models of the extent of OCSE in Cambodia without a larger nationally-representative study on prevalence, which would be likely to have significant limitations due to the often hidden nature of OCSE and lack of disclosure among its victims. Still, through the qualitative data gathered from learning workshops in this study, the learnings in the limited structured survey, and the review of reporting metadata, the study is able to construct a qualitative snapshot of the potential size of the issue in Cambodia and the extent to which children may be affected.

Learning workshops with children reveal that, out of the 220 child-participants in Phnom Penh, Siem Reap, and Sihanoukville, 37 children or 17% (about one-in-six children) shared at least one personal experience of OCSE-related risk on the internet. While this is not statistically representative, this does indicate potentially considerable risk among children in Cambodia. The majority, or 29 of these 37 children describe OCSE in the form of grooming or various forms of sexual advances by adults online— largely through Facebook or Facebook Messenger. Many of these sexual advances also include sharing sexually explicit materials or starting live video calls with the child.

While children in this study do not describe specific instances of systematic sexual exploitation and violence as has been found in the Philippines, there are still notable and widespread vulnerabilities to OCSE throughout all areas and among all groups of children in this project—

[63] Terre des Hommes-Netherlands. (2018).

particularly with regard to grooming and the production and distribution of Child Sexual Abuse Materials online. More research and further inquiry on the themes and patterns uncovered in this study should be conducted in order to better understand the experiences and vulnerabilities of Cambodian children on the internet.

Online surveys with children, although limited in scope, seem to indicate very similar findings, with 16% indicate feeling unsafe due to people online who ask them to do 'inappropriate things' and 19% who feel unsafe because of people who may circulate images of them online. Further, 13% cite sexual advances on social networking sites to be the biggest threats to their safety on the internet. Further, more than half of youth cite talking on the phone with someone that they had met online and nine youth (7%) indicate talking about sexual things with someone that they have met online. With regard to the availability of sexual images of children, nearly a third (32%) of youth in the online survey indicate seeing pornographic materials featuring children their age or younger while online.

Cambodian CSAM reports received by HSI in Phnom Penh have shown a steady increase from 2013 to 2017, however reporting from January to November 2018 shows a sharp and substantial increase of 490% with 123,896 CSAM reports in the first 11 months of 2018. More significantly, nearly a third of these reports (29% or 35,913) are considered to be new and actionable, potentially signaling an increase not only in the circulation of CSAM, but also in the potential production of new materials. There is a notable difference between OCSE-related reporting from NCMEC, APLE, and Child Helpline Cambodia (CHC). While NCMEC has processed more than 200,000 OCSE-related reports since 2015, APLE has processed 204, and CHC has processed seven within the same span of time. The stark differences between these mechanisms is due to the fact that reporting from NCMEC largely comes from US-based electronic service providers (such as Facebook), which are legally required to report any child abuse content that it reported on their platform or is discovered on their web servers. Whereas, APLE and CHC reporting solely relies upon public reporting, which requires the awareness and vigilance of the general Cambodian public.

## 6.3 What we have learned about our ability to address the issue

Learnings from workshops in communities, metadata from international monitoring organization, and data from online surveys have demonstrated significant clear vulnerabilities to OCSE in Cambodia throughout a variety of online platforms. In addition to this data, in-depth interviews with practitioners, and workshop data from children demonstrates a significant lack of issue awareness, monitoring, and supervision among parents and community members which may prevent instances of OCSE from being recognized and reported to local law enforcement or online reporting mechanisms, such as the APLE Internet Hotline. While there are a number of local and international capacities to respond to OCSE within the Cambodian government, such as the CyberCrime Unit and AHTJP, no single Cambodian agency is presently able to provide a full or sufficient response to OCSE.

**The CyberCrime unit**, under the Ministry of Interior, is a specialist unit which could potentially play a central role in responding to the mounting threat of OCSE in Cambodia. While this unit holds a broad mandate over the investigation of computer-related crimes in Cambodia (including crimes against children), their capacity for investigation is largely limited to searching physical electronic devices obtained during police investigations and lacks the ability to conduct online investigations. The lack capacity to directly investigate address internet-based crimes could render certain OCSE crimes committed on the Dark Web and through peer-to-peer networks invisible to local law enforcement. Further, the work of the CyberCrime unit, at present, is largely reactive, responding to inter-governmental referrals to investigate physical electronic devices as a part of criminal investigative work within local communities. There is a substantial need for a more proactive effort within the Cambodian government to work with

international and regional law enforcement to follow up on the mounting body of CSAM/CSEM reporting within Cambodia.

**The Anti-Human Trafficking and Juvenile Protection Department (AHTJP)** are tasked with responding to the threat of trafficking of children, and carries jurisdiction over various forms of sexual exploitation and violence against children both online and offline. With regard to OCSE, national law enforcement demonstrate a perpetrator-centered orientation to OCSE-related crime, which focuses more on identifying and prosecuting offenders that are physically present in Cambodian communities. Discussions about OCSE with law enforcement indicated a greater awareness of foreign offenders within local communities, who use the internet as a tool to meet with victims in an offline environment. However, this may overlook the majority of OCSE-related crime as perpetrators are often not physically located within the same country in which the victim is exploited. Within learning workshops several children indicate sexual advances from individuals believed to be located in a variety of different countries. Because perpetrators can be located in any number of counties, responding to OCSE-related crime requires strategic international alliances and collaborative agreements with international law enforcement (Interpol) in order to help keep children safe in local communities.

The current response to OCSE by local law enforcement is largely reactive to crime, responding to referrals from NGOs and other government agencies. However, public reporting and inter-agency referrals may only reflect an exceedingly small number of instances of OCSE. There is a need to become more proactive in investigating potential child-protection issues. There is a clear need and opportunity to work more closely with foreign investigators and international law enforcement agents on international CSAM/CSEM cases through the collaborative work surrounding the ICSE Database and actionable cases referred to US Homeland Security agents in Phnom Penh from NCMEC.

Internationally, there are a number of powerful resources that could potentially be available to Cambodian law enforcement, which could provide them with increased capacity to investigate internet-related crimes and provide the opportunity for practical capacity-building and investigative support.

**Interpol** is undertaking a substantial body of work on the issue of OCSE across the region through a collaborative effort using the ICSE Database. This can provide local law enforcement with a powerful resource to respond to the growing threat of OCSE in Cambodia. However, there is a substantial need for greater cooperation from ASEAN and East-Asian nations into the ICSE Database. Because the internet is a worldwide, decentralized, information network, the issue of online child sexual exploitation in Cambodia is also, by default, an international issue which requires an international response that is built upon a careful and strategic collaboration between local and international law enforcement.

At present the National Central Bureau in Phnom Penh (Interpol attached office in Cambodia) does not have direct access to international law enforcement efforts against CSAM/CSEM through the ICSE database. Because of this lack of collaboration, it is difficult to use this investigative tool to its fullest potential in Cambodia. Without a national-level connection the ICSE database (and its collaborative partners) international law enforcement face difficulties in understanding themes and patterns of OCSE offending in Cambodia. A formal collaboration between international and local law enforcement would help to ensure that all images CSAM/CSEM images uncovered within Cambodia are hashed, indexed, and access is given to international law enforcement. This would greatly benefit international victim identification efforts (including potentially thousands of unidentified Cambodian victims) by leveraging the local-level expertise offered by Cambodian law enforcement officials to help identify victims and prosecute offenders. At present, when CSAM discovered by police in the country, the full caches of confiscated images and related data are not being passed on to Interpol. Thus, local law enforcement in Cambodia are not able to benefit from the learnings and capacity-building offered by joining with the rigorous standards and processes of the international law enforcement community. In view of this, there is a need to establish a secure connection

between Phnom Penh NCB office and Interpol and to work toward enhanced collaboration with existing international initiatives and benefitting from their access to their specialized tool and resources.

**The National Center for Missing and Exploited Children (NCMEC)** provides a wealth of new and actionable cases of CSAM each month to the Homeland Security Investigations team at the US Embassy in Phnom Penh. However, in order to respond to active reports agents would need to work with Cambodian law enforcement and local ISPs to trace the offending IP address. This is very difficult within the Cambodian context as there is no standard for saving IP Assignment Logs. ISPs may save assignment logs for a matter of weeks, a matter of days, or even for just a matter of hours in some cases, making investigation of CSAM/CSEM reports virtually impossible. At present, there is no formal cooperative or response mechanism within Cambodia to receive, analyze, and process these leads coming from NCMEC through HSI. Such a cooperation would require a multidisciplinary commitment from HSI, local law enforcement, ISPs, and CyberCrime unit to follow up on reports and potentially open investigations on this rapidly growing stream of CSAM/CSEM reports coming from NCMEC.

# Chapter 7. Opportunities for Development

Any effective response to OCSE in Cambodia must be able to bring together a multi-stakeholder, interdisciplinary, and cross-sectoral national body of all entities that hold a responsibility to protect children in an online environment, including civil society and private industry. Such an effort should, ideally, be government-led and situated at the highest levels of national government and law enforcement. There is also significant need for this body to not only be a representative or legislative body, but also a practical one, with the capacity to develop adequate and responsive mechanisms to respond to OCSE more broadly, as well as CSAM/CSEM reporting from international entities such as NCMEC, while also proactively working monitor and safeguard children in an online environment. Such a body must be able to respond to the issue of OCSE holistically, addressing the various capacities defined in the WePROTECT Model National Response framework, as agreed by members of the Royal Cambodian Government in Abu Dhabi in 2015. While a full range of recommendations would need to be co-created with cross-sectoral government representation, some potential recommendations are defined below.

## 7.1. Policy and Governance

- **Complete and Ratify Cybercrime Legislation:** Cybercrime Law, which remains in draft form needs to be finalized to ensure full protection from OCSE including sextortion, sexting, live streaming, and online grooming. Possession of CSAM should be criminalized as a part of the new CyberCrime legislation. The adoption of this draft law should be accelerated.
- Develop a legislation to enforce this law.

In particular, this law should provide a basic offence for the possession child pornography for personal use and address the distribution, sale, lease, displaying, projection or presentation of pornography in private places—not only in public places.

These are significant gaps in present legislation. The extent of this term would need to be carefully defined under Interpol CSAM guidelines, so as to be thoroughly contextualized for the Cambodian context to avoid unnecessary prosecution of individuals.

- **Develop ISP Legislation to Set Standards for IP Assignment Log Preservation:** Based on Cambodia laws, should identify the guideline and standard to records IP data (IP Assignment Log Preservation) required to all of internet service to establish child protection within quick respond with high commitment on CSAM content in Company servers. Over the past six years, there has been a substantial increase in new and actionable reporting on Cambodian CSAM/CEM to HSI in Phnom Penh from NCMEC. However, developing this reporting into actionable intelligence has been made nearly impossible due to the fact that there is no set standard of time for Cambodian ISPs to maintain IP assignment logs, which are central to this process. Thus, the Royal Cambodian Government should immediately put forth a set of standards by which such vital records can be preserved.
- **A mechanism should be established (as committee or working-group)** with involvement from ministry, which is MoI, MoPCT, MoEYS, Ministry of Culture, MoJ, MoSVY, MoIn, MoWA is specifically working on the OCSE in timely manner.
- Exchange visit to learn and sharing an experience on effectives OCSE.
- **Amend Current Telecommunications Legislation to Prevent OCSE:** An amendment to Law on Telecommunication should be added to integrate the prevention and protection of Online Sexual Exploitation. This should include the establishment of child-protection policies to require all ISPs to take action and responsibility for CSAM content

hosted on their servers and impose strict penalties against ISPs which fail to follow/implement these laws and policies.

# 7.2 Internet Service-Industry

**1. Ministry of Post and Telecommunication- Acceleration level response to CSAM**:

- To develop clear procedures and allocate sufficient resources to the prompt identification, reporting, and take-down of CSAM identified on Cambodian servers. When CSAM is identified that is hosted in another country, ISPs and the Ministry of Telecom should have processes in place through which they can work collaboratively to block or filter access to the material while the international host is contacted and given the ability to respond.
- Ministry of Culture and Arts, MoWA, and other relevant line ministry should develop the common guideline to identify the illegal contents on CSAM internet posted or social media that significant effect to religions and cultures.

**2. Developing issue-awareness and fostering a sense of urgency to respond:**

- Educated of the impact of CSAM and CSAM cases respond timely (both government and industry).
- It is important that local industry, along with the Cambodian government, take personal responsibility to see that CSAM involving Cambodian children is addressed promptly and with urgency, even if the material is not hosted on Cambodian servers. Both industry and the Cambodian government should be made aware of the impact of allowing CSAM to remain on servers, both on the child victim who is re-victimized every time the image is viewed, as well as the impact on disrupting the offender's ability to access and further distribute the materials.
- Increase the dissemination and mainstreaming of crime awareness and risks of technology.
- Develop a poster or video sport for educated on CSAM (Respond by CNCC and MoI).

**3. Emphasizing Corporate Social Responsibility**:

It is important for national mechanisms to actively address the issue of OCSE on multiple fronts, including the development of child-protection partnerships within the financial sector, creating awareness around the various payment systems used to compensate producers of CSAM, including services such as Western Union, Wing, Cryptocurrency, and other anonymous forms of sending money. Developing partnerships with such private industries not only allows deeper penetration of the issue, but can also be integrated into existing mandates for corporate social responsibility within the private sector.

- Stimulate and encourage internet service companies provide clear instructions to clients on how to use the internet safe for children (Parental control).
- Stimulate and encourage the internet service companies would be have a possibilities to control and signal against the use of pornography or child pornography website.

# 7.3 Criminal Justice

- Expansion the anti-cybercrime networking at sub-national levels to prevention, protection and respond to CSAM timely.
- **Investment in and development of the CyberCrime Unit:** Efforts should be made to significantly develop the CyberCrime unit, allowing for more proactive monitoring and response at a community level. It is important that local communities are aware of

existing resources and child-protection units that are available to provide a specialized response to child protection risks online. At present, the CyberCrime Unit is a small team with a broad mandate covering a range of computer-related crimes. Because of this broad mandate, international child protection advocates indicate the team lacks the bandwidth to address online child protection concerns. Thus, it could be helpful to hire and train specialized child-protection officers that are able to proactively collaborate with police, civil society, US Homeland Security, and other relevant partners to process cases, build intelligence, and conduct specific investigations— especially with regard to existing cases referred through US homeland security through NCMEC.

- **Support for the development of a practical-response task force**: Over the past six years, there has been a steady increase of OCSE reporting to HSI in Phnom Penh, especially for the year 2018. Developing these reports into actionable intelligence requires a proactive, multi-stakeholder team of agents that are able to act on critical or high-priority reports in order to identify perpetrators and protect victims. Thus, there is a need for the establishment of a practical body or taskforce, which would be able to bridge the gap between US Homeland Security (the body receiving the NCMEC referrals), the local Cambodian Cybercrime Unit, and Internet Service Providers in order to coordinate the investigation and prosecution of CSAM referrals. This would include the establishment of a VPN system under Cambodian government to receive and follow up on high-priority NCMEC leads, in collaboration with HSI, FBI, and international law enforcement (Interpol). Developing such a collaboration would allow members of Cambodian criminal justice to not only be able to receive reports of OCSE from international law enforcement (Interpol), NGOs (such as APLE Internet Hotline), and industry (such as NCMEC) reporting, but also to be able to develop these reports into actionable intelligence to enable investigations to be undertaken.
- **Developing closer working relationships with international law enforcement:** The exchange of CSAM online is a multi-jurisdictional issue which requires law enforcement to cooperate at both national and international levels to share information and intelligence (WeProtect, 2018). Data from this study indicates an immediate need to establish a secure connection between Phnom Penh NCB office and Interpol, which would aid in unifying the process of dealing with CSAM to ensure that all images are hashed, indexed, and access is given to international law enforcement. As a part of this, national police would need to unify their processes and standards for dealing with caches of CSAM, across the country to comply with international standards.

There is a further need for Cambodian Law Enforcement to establish an official connection with the ICSE Database. In order for Interpol to consider for such a connection, the Cambodian government would first need to establish a dedicated law enforcement unit/team for child sexual abuse and exploitation, include legislation that penalizes the production, possession and/or distribution of child sexual abuse material, and be able to provide sufficient bandwidth and needed cyber-security to support connection to the ICSE database. While developing this connection would require a significant amount of work, such a connection would greatly enhance the operational capability of Cambodian law enforcement and allow for instant local access to the data and tools required for uploading and analyzing CSAM seized by law enforcement around, greatly aiding Cambodian Law Enforcement in the process of identifying victims and offenders throughout the nation.

- **Capacity-building of law enforcement**: National Law Enforcement in Cambodia must be provided with the knowledge, skills, systems, tools, and resources needed to conduct investigations and utilize specialized intelligence within an online environment. This could be provided through increased collaboration with international law enforcement (Interpol). It is important for national law enforcement to maintain a strong focus on supporting and protecting victims and ensuring that investigations are undertaken using leading child-protection principles. At present, law enforcement seem to take a perpetrator-centered approach to child-protection in online environments. While

investigating perpetrators is important, as crimes increasingly move into a digital environment, it is vital for police to understand OCSE as a multi-jurisdictional issue. This may require significant international cooperation to investigate and prosecute perpetrators that are not based within the same country as the victim.

# 7.4 Societal

1. **OCSE Awareness and Training for end-users:** Student and teacher data from learning workshops consistent emphasizes the need for online safety training and issue-level awareness raising around OCSE. In particular, children and their parents/caretakers need training on how to use social media privacy settings to keep their pictures and personal information safe, how to set a stronger password to protect users' accounts, and how to understand and avoid the practices of online predators. This includes training on how to report risky or abusive content to social media platforms, so that appropriate actions can be taken. Further, Children cite the importance of knowing local resources to report abuse, such as APLE Internet Hotline and the Cambodia Child Helpline (1280). They indicate that services such as these are vital because they provide social workers with a safe platform where they can report risks and have access to important resources to protect their privacy and find solutions to online risk.

   Programming such as this should be developed at the national level to ensure consistency in messaging and that it is delivered to all areas and contextualized to local communities. Ideally, programming such as this should be integrated into national curriculum to ensure widespread coverage. Curriculum such as this could potentially be incorporated into related educational programming on sex and relationships. Existing best practice resources can be utilised from various international stakeholders, but it is important for these to be contextualized to ensure they are relevant for local Cambodian communities in both rural and urban contexts.

2. **Social media training for parents and greater engagement with children:** Teachers and students indicate the need for parents to be more aware of their children's online environments and more greatly engaged with their children's lives on the internet. While teachers cite this as a need for child safety, children in learning workshops also seem to welcome the idea of positive parental engagement into their digital world.

   - As a part of this, children in learning workshop encourage engagement from civil society and private industry to address this issue by developing public awareness campaigns for TV and within schools to communicate the potential dangers online, and providing training for end-users on how to protect from various online predators.

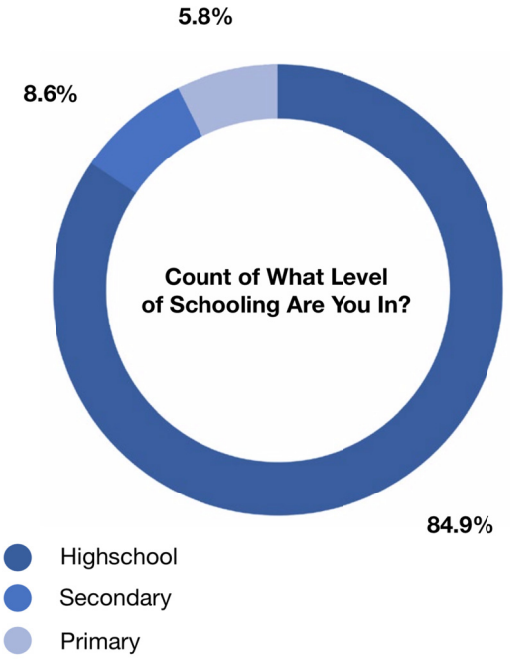
   - **More accessibility for Internet Hotlines:** Children indicate that the resources provided by services such as APLE Internet Hotline are important, it is vital that Child Helplines such as these are more widely known and easy to use for children, parents, and child advocates at the community level. Throughout this situational analysis children and youth have demonstrated OCSE to be a significant risk within their online environments, which seems to be supported by the influx of Cambodian CSAM/CSEM reporting from social media platforms through NCMEC. Despite this reality, only 204 OCSE-related cases have been reported to APLE internet hotline since 2015, and seven have been reported to Child Helpline Cambodia. The success of child helplines relies open public reporting, which requires awareness and vigilance among the general public. Thus it is important that the existence of these resources are emphasized as a part of child protection training in NGOs and in schools. Further, it is important that awareness campaigns for these resources are consistently improved upon and reporting platforms are made more user-friendly to allow for easier reporting.

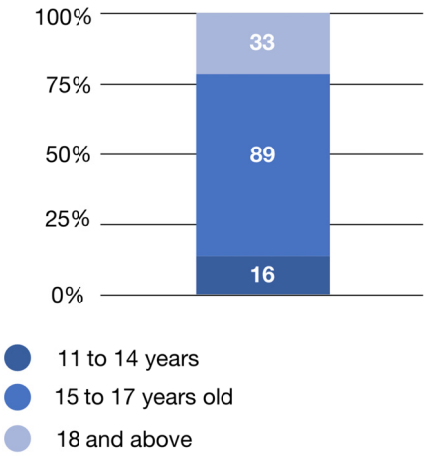
- **Child participation in the development of interventions and initiatives:** Children and young people should be respected as the 'experts' of their own online environments and should be encouraged and enabled to give their ideas and influence the development of OCSE-related policy and practice nationwide. Thus, any national initiative or plan of action for children should be developed with significant direct input and interaction with children themselves. Children in learning workshops consistently demonstrated a significantly more nuanced and thoughtful understanding of the vulnerabilities that they faced within their online environments and various ways in which these environments could be made safer within the Cambodian context. Thus, it is important for the national government to place a greater value on the voices of children and acknowledge the vast resource of practical knowledge that they offer to this issue.

# Annex 1: Structured Surveys

The initial intention of this section of the situational analysis was to collect a limited, but nationally-representative sampling of Cambodian youth in public, private, and alternative schools. However, due to time and political constraints, the breadth of survey was limited to a significantly smaller sampling of public school youth within one geographic area of Cambodia. While the data provided here is in no way representative of the nation as a whole, it can still offer a useful set of learnings about internet use among this particular group of youth and provide a helpful comparison to the learnings developed in the workshops conducted with children in Phnom Penh, Siem Reap, and Sihanoukville. In total, the research collected 139 online surveys, which were disseminated to computer classes among public school youth in Battambang.

## Demographics

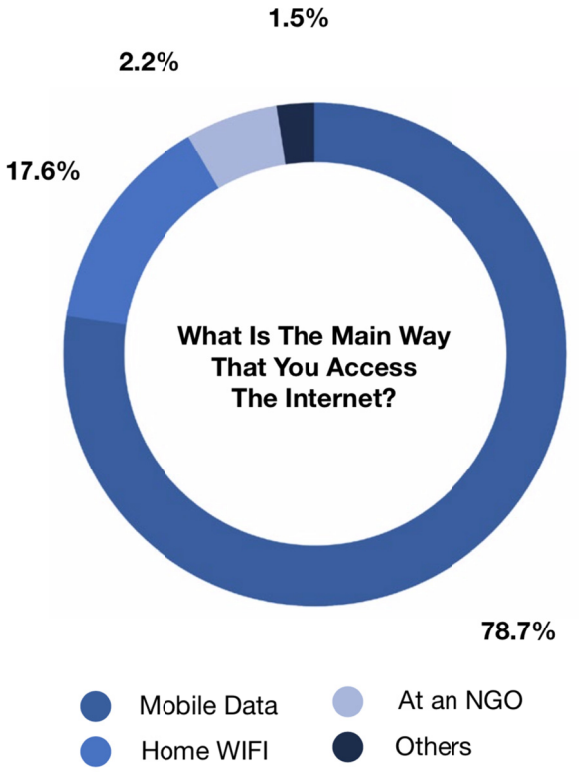



Among the 139 youth surveyed, the majority, or 89 (64%), were 15 to 17 years of age, while 33 (23.7%) were 18 to 20 years of age and 16 (11.5%) were between the ages of 11 and 14. Only one respondent cites being between the ages of 8 and 14. The vast majority (84.9%) are enrolled in High School, while the remaining 14.4% were in either primary or secondary education. All but two respondents (137) attend a public school and the remaining students attend alternative, or NGO-based, schools.

## Internet Use

Use of mobile internet services on a smartphone was, by far, the most common means of connecting to the internet for students, cited by 107 or 79% of the 136 students responding to this question. Apart from mobile services, approximately one-in-six students (24 or 18%) cite connecting to the internet through a Wifi connection at home, three students (2%) cite most commonly connecting to the internet most at an NGO and two students (1%) cite connecting to the internet through public Wifi.




The majority of students (71 or 65%) cite spending less than three hours a day on the internet with 29% spending less than one hour and 36% spending between one and three hours on the internet. To a lesser extent, 17 students (12%) cite spending more than three hours a day on the internet, eight of which (6%) cite spending more than 5 hours on the internet. Lastly, 5 or 4% cite that they are not sure how much time that they spend online. A report on internet use among young Cambodians cites similar findings with 49% of young internet users using the internet for more than 30 minutes a day.

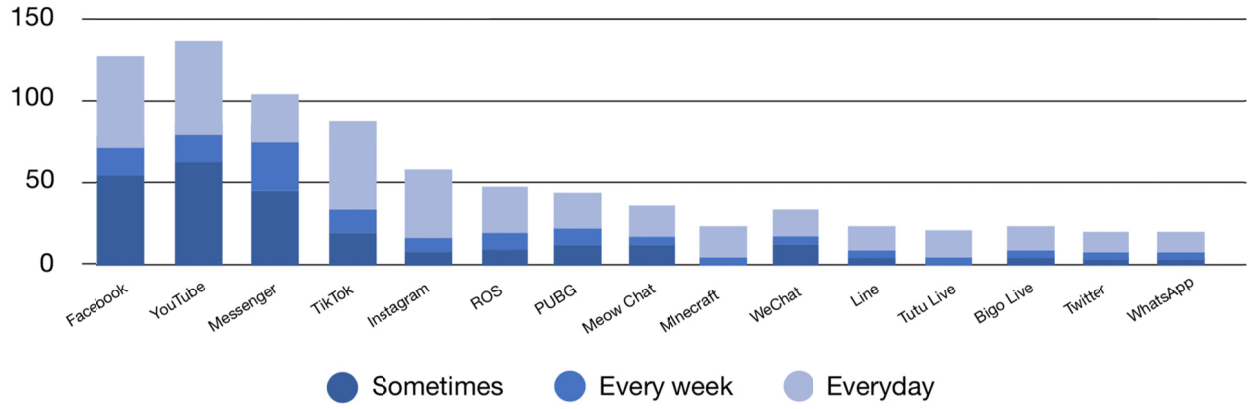
Parents are cited to provide the majority of students (82 students or 59%) with money to connect to the internet, largely through paying for mobile internet, while nearly one-in-six students (24 or 17%) cite paying for the internet with their own money. To a lesser extent, six students cite connecting to the internet through an NGO and two cite receiving money from others for their internet connection.

## Reasons for Using the Internet

Students were asked to consider the primary and secondary reasons that they usually connect to the internet. More than two-thirds of students (92 or 67%) cite that the primary reason that they connect to the internet is for their studies and 52 students (41%) cite that their studies is the secondary reason that they go online. Notably, 41 students (30% of students indicate "homework") as both the primary and secondary reason that they usually connect to the internet.

Given that the online survey was administered within the context of school classrooms, it is possible that respondents would be more likely to indicate “studies” as a primary or secondary reason for connecting to the internet, than if the survey were administered in a non-scholastic context, such as an internet cafe or on a social media platform. Apart from their studies, primary reasons for connecting to the internet include 18 or 13% of students who cite going online to the internet to watch videos, followed by downloading files and videos (8 or 6%), playing games (6 or 4%), and social media (4 or 3%), among other reasons (10 or 7%). Secondary reasons for connecting to the internet, following studies, include downloading files and videos (25 or 18%), watching videos (25 or 18%), social media (12 or 9%), and playing games (11 or 8%), among others (8 or 6%).

## Apps used and Frequency of Use




Seemingly contradictory to the student's stated reasons for connecting to the internet, respondents indicate regular and frequent use social media and video streaming services while they are on the internet. Most commonly used is Youtube, Facebook, and Facebook Messenger, which are used by 89%, 94%, and 75% of youth, respectively. TikTok, a live-streaming music app, is also commonly cited by 84 youth or 60%. Gaming apps, such as Rules of Survival, PUBG, and Minecraft are used by a minority of students, cited by 31%, 28%, and 16%, respectively. The findings here are consistent with patterns of app usage in the learning workshops in Siem Reap, Sihanoukville, and Phnom Penh, as well as media research conducted by UNDP, which cites that young people use internet for reading news (73%) and their daily access is more than to the traditional forms of media (66%), social networks (63%), general web browsing (42%), playing games (31%), studying and reading (30%), and watching TV and movies (27%).[64]

Considering the four most commonly used apps (Youtube, Facebook, Facebook Messenger, and TikTok), Youtube is the most commonly used among youth, as well the app which is used the most regularly with 42% using it every day, and 56% using it every week. Males and females both use YouTube at similar rates, however, males are slightly more likely to be regular users (55% of males indicating daily or weekly use, in comparison with 43% among females). More than half (56%) of 11 to 14 year olds, and nearly two-thirds (64%) of 15 to 17 years, use YouTube either daily or weekly. YouTube is used to a lesser extent (36%) among youth 18 and older. Findings here are consistent with the aforementioned report by UNDP, which finds the most two popular apps are Facebook (79%), followed by YouTube (63%) among its sample of Cambodian young people with internet access.

With regard to Facebook, the social media app is used, overall, more commonly than its messaging app, 'Messenger' (89%, in comparison with 75%), however, among regular users, the messaging app is used with a similar frequency (46% and 47%, respectively). With regard to age, the majority of regular Facebook users are between the ages of 15 and 17 years. More than half (53%) of 15 to 17 year-olds use Facebook either daily or weekly. To a lesser extent, 31% of 11 to 14 year-olds and 36% of youth 18 or older use Facebook either every day or on a weekly basis. No significant differences are notable between male and female users.

Considering Messenger, Facebook's messaging app, students 15 to 17 years of age indicate more regular use of Messenger with 57% indicating use of the app either every day or every week. In comparison, more than a third of 11 to 14 year-olds (37.5%) and 27.2% of youth 18

[64] UNDP. (2014), 24.

and older indicate daily or weekly use of the app. No significant differences are notable between male and female users (51% among males and 49% among females).

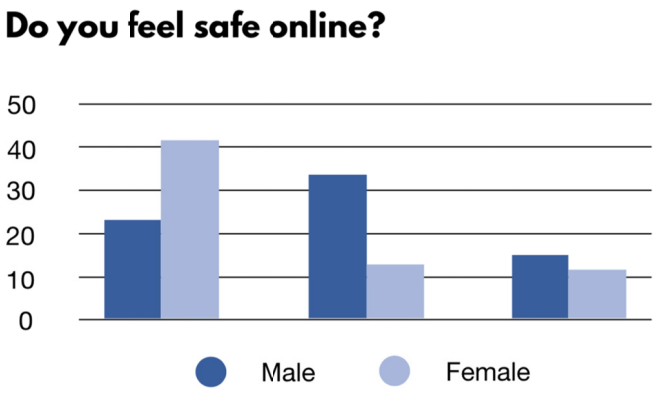
## Parental Involvement and Supervision

Youth were asked about the extent to which they talk with their parents or carers about what they do on the internet. While the majority of the youth (102 or 75%) indicate that they do communicate with their parents about what they do on the internet, one-in-four youth cite that they do not generally communicate with their parents about their online activities. Specifically, 20 of the 139 youth, or 15% cite that they rarely communicate and 15, or 11%, cite that they never talk to their parents about their online activities. Males were slightly more likely to cite communicating with their parents in comparison with females with 77% of males and 71% of females talking with parents “often” or “sometimes” about their online activities.

The majority of youth (74 or 53%) cite that they are not given any restrictions on their internet use. Among the 47% of youth who do have some form of limitation or restriction on their online activities, 19% cite having limitation on the time that they spend on the internet, 18% cite that their parents restrict the content that they are able to access, and 9% indicate having restrictions on both time and content. Females were notably more likely to have restrictions placed on their online activities in comparison with males, with 55% of females and 40% of males having some form of restrictions in place.

## Risky Experiences Online

Only a minority of youth, or one-in-five (20%), indicate that they feel safe while they are online. More than one-in-four (27%) cite that they do not feel safe online and the majority, or 54%, cite that they "sometimes" feel safe online. Males are more than twice as likely to feel safe online in comparison to females (47% of males, in comparison to 21% of females). However, females were only slightly less likely to cite feeling unsafe while on the internet with 18% of females feeling unsafe and 21% of males indicating that they feel safe online. While these differences are of note, it should also be considered that the differences of 'feeling' safe online may not necessarily reflect their actual experience of risk or safety online, but rather could reflect the youth’s gender socialization, which commonly assumes females to be more vulnerable and males to be more resilient.

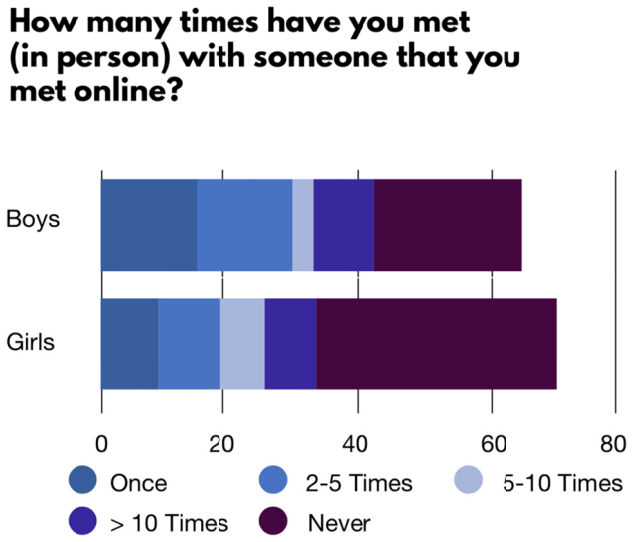



Youth indicate a number of online experiences that make them feel unsafe which are consistent with OCSE. One-in-six youth (19%) indicate feeling unsafe due to (or fears of) people online who will use images of them and circulate them online. Nearly one-in-five youth (16%), indicate feeling unsafe due to ‘people online who ask me to do inappropriate things’. Further, 13% of youth indicate feeling unsafe because of seeing violent images, and another 13% cite feeling unsafe due to seeing sexual images while they are online. In addition to potentially OCSE-related factors, internet scams or being cheated out of money are the most common reason that youth feel unsafe on the internet, cited by nearly one-in-three youth. Nearly one-in-four youth (23%) cite that they feel unsafe due to bullying or harassment from people online.

The majority of youth (57%) cite that they have seen pornographic images on the internet, which is notably more common among males (67%, compared with 46% among females. Most notably, 11 of the 17 young respondents (8-14 year olds) cite seeing pornographic images on the internet. While this is a small sample of youth, it is significant that a greater proportion of younger respondents (11 of 17 youth) cite seeing pornographic materials online in comparison to older youth 67 of 121 youth).

Notably, among the youth who cite seeing pornographic materials online, 32% indicate that they have seen pornographic materials featuring youth that were their age or younger. An additional 49% cite that they are unsure if they have seen pornographic materials featuring youth their age or younger. Only one-in-five youth who have seen pornography cite that they have not seen pornographic materials featuring youth their age or younger. While these findings are in no way conclusive, further research is needed to understand the various content that young internet users are exposed to in Cambodia.

One-in-five youth (20%) indicate having added a stranger to a social networking friends list, with similar rates indicated among males and females. While only 20% of youth indicate adding a stranger online, more than half (51%) cite talking on the phone with someone that they had met online, with 26% or 35 youth doing this "once", 14% or 19 youth doing this two to five times, 5% or 7 youth doing this 5 to ten times, and 7% or nine youth doing this more than ten times. Among those who have spoken or chatted with someone that they met online nine youth indicate talking about sexual things with the person that they had met, with similar findings among both males and females. Meeting in-person with someone that the youth had met online was common with 88% of boys and 60% of girls (or 73% of all youth) indicating that they had met in-person with someone they had met on the internet at least once. Among all youth, 29 or 27% cite doing this once, 26 or 28% cite doing this two to five times, seven or 7% cite doing this five to ten times, and 14 or 13% cite doing this more than ten times. While the circumstances of these meetings are unclear and much more research is needed into the online practices of youth in Cambodia, these findings seem to indicate a potentially significant need for safer online practices.




| What do you think is the biggest threat when you go online? | | |
|---|---|---|
| Someone using my photos in an inappropriate way | 33 | 24.09% |
| Bullying or harassment by friends or acquaintances | 32 | 23.36% |
| Bullying or harassment by strangers | 31 | 22.63% |
| Unwanted sexual approaches in a chat room, social networking site or on email | 18 | 13.14% |
| Seeing sexual images or content | 18 | 13.14% |
| Someone taking unwanted photos of me and circulating them | 17 | 12.41% |
| Threats in the place/environment where I access the Internet | 9 | 6.57% |

| | | |
|---|---|---|
| I don't think there are many risks | 28 | 20.44% |
| Other | 8 | 5.84% |

Youth were also asked to reflect on what they experience on the internet and indicate what they believe to be the biggest threat to their safety. OCSE-related threats are commonly indicated throughout responses to this question. Most commonly, youth indicated that people who use their photos in an inappropriate way was the biggest threat when they went online, cited by 33 youth or 24% of respondents. Similarly, 17 or 12% of youth indicate threats of having unwanted photos taken of them and circulated on the internet and to a lesser extent, 18 youth (13%) indicated threats of unwanted sexual approaches, 18 (13%) indicated threats of seeing sexual content. Other threats, which are not necessarily related to OCSE include various forms of bullying online, with 32 (23.4%) citing bullying from friends or acquaintances and 31 (22.6%) indicating bullying or harassment from strangers. Further, nine youth or 6% cite environmental threats in the place where they accessed the internet— a theme which is also common among youth from vulnerable communities within the learning workshops conducted in Phnom Penh, Siem Reap, and Sihanoukville. Lastly, one-in-five youth (28 or 20%) didn't believe that there are many threats to their safety when they went online.

Overall, youth participating in the structured surveys indicate notable risks on a variety of fronts, including seeing sexual content featuring both adults and other children, as well as encounters with people that they indicate having met online. Further, youth indicate a variety of vulnerabilities, not only with regard to breaches of their privacy and other OCSE-related risks, but also with regard to cyber-bullying.

# Bibliography

Action Pour Les Enfants Cambodia (2016). Roundtable Meeting on Online Sexual Exploitation of Children and Abuse. Meeting Minutes, Phnom Penh.

Action Pour Les Enfants Cambodia (2018). Current Perception of Child Sexual Abuse and Exploitation in Cambodia: A Study in Five Provinces. Action Pour Les Enfants: Phnom Penh.

Chan, S. (2018, June 27). Government issues final deadline to register SIM card users. Retrieved August 14, 2018, from https://www.khmertimeskh.com/50505669/government-issues-final-deadline-to-register-sim-card-users/

Craven, et al., (2006). An international, interdisciplinary forum for research, theory and practice, Vol. 12, Issue 3. Sexual grooming of children: Review of literature and theoretical considerations. Retrieved from: https://www.tandfonline.com/doi/abs/10.1080/13552600601069414

ECPAT International (2016). Offenders on the move. Global Study Report on Sexual Exploitation of Children in Travel and Tourism. ECPAT International: Bangkok. Retrieved February 20, 2017 from http://globalstudysectt.org/global-report/

ECPAT International (2017). Online Child Sexual Exploitation: A Common Understanding. ECPAT International: Bangkok. Retrieved January 12, 2018, from: http://www.ecpat.org/wp-content/uploads/2017/05/SECO-Booklet_ebook-1.pdf

ECPAT International, & INTERPOL. (2018). Towards a Global Indicator on Unidentified Victims in Child Sexual Exploitation Material. Retrieved March 9, 2018, from http://www.ecpat.org/resources/towards-global-indicator-unidentified-victims-child-sexual-exploitation-material-summary-report/

Elliot, I.A., & Ashfield, S. (2011). The use of online technology in the modus operandi of female sex offenders. Journal of Sex Aggression, 17(1), 92-104.

European Union Agency for Law Enforcement Cooperation (Europol, 2017). Internet Organised Crime Threat Assessment.

Hurley, R., Wolak, J., Prusty, S., Soroush, H., Walls, R. J., Albrecht, J., Lynn, B. (2013). Measurement and analysis of child pornography trafficking on P2P networks. Proceedings of the 22nd International Conference on World Wide Web - WWW'13. doi:10.1145/2488388.2488444

INHOPE (2016). Facts, Figures & Trends 2016. The fight against online Child Sexual Abuse in perspective. Retrieved from: http://www.inhope.org/tns/resources/statistics-and-infographics/statistics-and-infographics-2016.aspx

Interagency Working Group on the Sexual Exploitation of Children (2016). Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse. Retrieved February 10, 2016 from http://luxembourgguidelines.org

Kierkegaard, S. (2008). Cybering, Online Grooming, and Age play. Computer Law and Security Report, 24, 41–55.

Kloess, J. A., Beech, A. R., & Harkins, L. (2014). Online Child Sexual Exploitation. Trauma, Violence, & Abuse, 15(2), 126-139.

LIRNEasia (2018). After Access: ICT access and use in Cambodia and the Global South, Phnom Penh, Cambodia.

McAlinden, A-M. (2006). "Setting 'em up": Personal, familial and institutional grooming in the sexual abuse of children. Social and Legal Studies, 15(3), 339-362.

Ministry of Women's Affairs. National Action Plan to Prevent Violence Against Women, 2014-2018. Retrieved from: http://cambodia.unfpa.org/sites/asiapacific/files/pub-pdf/NAPVAW2014-2018%28Eng%29.pdf Accessed 21 June 2016

NetClean. (2017). The NetClean Report 2017. Retrieved December 14, 2018, from https://www.netclean.com/netclean-report-2017/download/

OHCHR (2016). New digital technologies produce unprecedented levels of child abuse material online. Retrieved July 30, 2016 from: http://www.ohchr.org/EN/NewsEvents/Pages/Childsexualexploitationonlineontherise.aspx

Steel, C. M. S. (2009). Child pornography in peer-to-peer networks. Child Abuse & Neglect, 33(8), 560–568. doi:10.1016/j.chiabu.2008.12.011

Terre des Hommes-Netherlands. (2013). Full screen on view: An exploratory study on the background and psychosocial consequences of Webcam Child Sex Tourism in the Philippines. The Hague, Netherlands.

Terre des Hommes-Netherlands. (2014). Webcam Child Sex Tourism, Becoming sweetie: A novel approach to stopping the global rise of Webcam Child Sex Tourism. The Hague, Netherlands.

Terre des Hommes-Netherlands. (2016). Children of the Webcam: Updated report on webcam child sex tourism. The Hague, Netherlands.

Terre des Hommes-Netherlands. (2018). Live-Streaming Online Child Sexual Exploitation in the Philippines (Regions III and VII). Phnom Penh, Cambodia.

UNDP (2014). Youth in Cambodia: Media Habits and Information Sources. Retrieved from: http://www.kh.undp.org/content/dam/cambodia/docs/DemoGov/Media%20Habits%20and%20Information%20Sources%20of%20Youth%20in%20Cambodia.pdf

UNICEF (2016). Victims are not Virtual: Situation assessment of online child sexual exploitation in South Asia. Retrieved from https://www.unicef.org/rosa/Victims_are_not_virtual.pdf

UNICEF (2017). Child Privacy in the Age of Web 2.0 and 3.0: Challenges and Opportunities for Policy. Retrieved from: https://www.unicef-irc.org/publications/926-child-privacy-in-the-age-of-web-20-and-30-challenges-and-opportunities-for-policy.html

US Department of Justice; INTERPOL (2018). Tackling child sexual abuse focus of INTERPOL experts meeting. Retrieved from https://www.interpol.int/News-and-media/News/2018/N2018-141

We Are Social (2017). Digital in 2017: South East Asia. Retrieved from https://www.slideshare.net/wearesocialsg/digital-in-2017-southeast-asia.

WePROTECT (2016). Preventing and Tackling Child Sexual Exploitation and Abuse (CSEA): A Model National Response.

World Bank (2015). Protecting Children from Cybercrime: Legislative responses in Asia to fight child pornography, online grooming, and cyberbullying. Retrieved from http://documents.worldbank.org/curated/en/652251468206670506/pdf/94492-WP-REVISED-PUBLIC-Box385442B-Protecting-Children-from-Cybercrime-Legislative-Responses-in-Asia-to-Fight-Child-Pornography-Online-Grooming-and-Cyberbull.pdf.

---