DISRUPTING HARM IN VET NAM [SNAPSHOT]

Evidence on online child sexual exploitation and abuse

Funded by

End Violence Against Children Implemented by







Warning:

Disrupting Harm addresses the complex and sensitive topic of online child sexual exploitation and abuse. At times in the report, some distressing details are recounted, including using the direct words of survivors themselves. Some readers, especially those with lived experiences of sexual violence, may find parts of the report difficult to read. You are encouraged to monitor your responses and engage with the report in ways that are comfortable. Please seek psychological support for acute distress.

Suggested citation:

ECPAT, INTERPOL, and UNICEF. (2022). *Disrupting Harm in Viet Nam [SNAPSHOT]: Evidence on online child sexual exploitation and abuse.* Global Partnership to End Violence Against Children.

Copyright © ECPAT, End Violence Partnership, INTERPOL, UNICEF, 2022. Use of this publication is permitted provided the source is acknowledged and that the publication is not used for commercial purposes.

Funding from the Global Partnership to End Violence Against Children, through its Safe Online initiative, does not constitute endorsement.

Note from the End Violence Partnership	4
Executive summary	6
<i>Disrupting Harm</i> methods	11
About online child sexual exploitation and abuse	15
About Viet Nam – demographics and internet usage	18
Overview of legislation and policy	22
1. Children Online in Viet Nam	25
1.1 Internet access and barriers	26
1.2 Children's activities online	29
1.3 Perceptions and experiences of risky online activities	30
2. Online Child Sexual Exploitation and Abuse in Viet Nam	39
2.1 Law enforcement data	41
2.2 Children's experiences of child sexual exploitation and abuse in Viet Nam	48
2.3 Other experiences of children that may be linked to OCSEA	53
3. Responding to Online Child Sexual Exploitation and Abuse in Viet Nam	55
3.1 Formal reporting mechanisms	56
3.2 Law enforcement response	59
3.3 Going to court and accessing services	62
3.4 Coordination and collaboration	65
4. How to Disrupt Harm in Viet Nam	69
4.1 Four key insights and recommendations for actions	70
Acknowledgements	75

Our online lives are advancing constantly. The internet and rapidly evolving digital communication tools are bringing people everywhere closer together. Children are increasingly conversant with and dependent on these technologies, and the COVID-19 pandemic has accelerated the shift online of many aspects of children's lives.

The internet can be a powerful tool for children to connect, explore, learn, and engage in creative and empowering ways. The importance of the digital environment to children's lives and rights has been emphasised by the United Nations' Committee on the Rights of the Child in <u>General Comment No. 25</u> adopted in 2021. The General Comment also stresses the fact that spending time online inevitably brings unacceptable risks and threats of harm, some of which children also encounter in other settings and some of which are unique to the online context.

One of the risks is the misuse of the internet and digital technologies for the purpose of child sexual exploitation and abuse. Online grooming, sharing of child sexual abuse material and live-streaming of child abuse are crimes against children that need an urgent, multi-sectoral and global response. These crimes are usually captured in permanent records in the form of digital images or videos, and are perpetually reshared online, victimising children over and over again. As risks of harm continue to evolve and grow exponentially, prevention and protection have become more difficult for governments, public officials, and providers of public services to children, but also for parents and caregivers trying to keep-up with their children's use of technology.

With progress being made towards universal internet connectivity worldwide, it is ever-more pressing to invest in children's safety and protection online. Governments around the world are increasingly acknowledging the threat of online child sexual exploitation and abuse, and some countries have taken steps to introduce the necessary legislation and put preventive measures in place. At the same time, the pressure is mounting on the technology industry to put the safety of children at the heart of design and development processes, rather than treating it as an afterthought. Such safety by design must be informed by evidence on the occurrence of online child sexual exploitation and abuse; Disrupting Harm makes a significant contribution to that evidence. The Global Partnership to End Violence against Children, through its Safe Online initiative, invested US\$ seven million in the *Disrupting Harm* project. *Disrupting Harm* uses a holistic and innovative methodology and approach to conducting comprehensive assessments of the context, threats and children's perspectives on online child sexual exploitation and abuse. This unprecedented project draws on the research expertise of ECPAT, INTERPOL, UNICEF Office of Research – Innocenti, and their networks. The three global partners were supported by ECPAT member organisations, the INTERPOL National Central Bureaus and the UNICEF Country and Regional Offices. It is intended that the now developed and tested methodology is applied to additional countries around the world.

Disrupting Harm represents the most comprehensive and large-scale research project ever undertaken on online child sexual exploitation and abuse at a national level and has resulted in 13 country reports and a series of unique 'data insights'. It provides the comprehensive evidence of the risks children face online, how they develop, how they interlink with other forms of violence and what we can do to prevent them.

The findings will serve governments, industry, policy makers, and communities to take the right measures to ensure the internet is safe for children. This includes informing national prevention and response strategies, expanding the reach of Disrupting Harm to other countries and regions, and building new data and knowledge partnerships around it.

Disrupting harm to children is everyone's responsibility.

Dr Howard Taylor Executive Director End Violence Partnership

EXECUTIVE SUMMARY

Funded by the Global Partnership to End Violence Against Children, through its Safe Online initiative, ECPAT, INTERPOL and UNICEF Office of Research – Innocenti worked in partnership to design and implement a multifaceted research project on online child sexual exploitation and abuse: *Disrupting Harm*. The research was conducted in seven Eastern and Southern African countries and six Southeast Asian countries, including Viet Nam.

In Viet Nam, only four out of the nine Disrupting Harm research activities were implemented: a nationally representative household survey was carried out with children aged 12–17 and one caregiver of each child; written interviews were conducted with police units; crime data were analysed, and global hotlines and helplines provided data to complement the law enforcement data. Due to complex government regulations, permission to conduct contextualising research activities was not forthcoming after nine months and consequently interviews could not be conducted with children and caregivers who had accessed the justice system or with justice professionals and key government representatives with mandates relevant to online child sexual exploitation and abuse (OCSEA). A survey of frontline social support workers was also not possible. Consequently, while this report describes children's experiences of OCSEA as captured in the household survey and provides an overview of law enforcement data, it does not contain information about how the national legal systems are operating to respond to these crimes, nor does the data allow for deeper insights into children's experiences of accessing support or capture the perspectives of the child protection workforce. This limits the extent of the recommendations made.

Please see figure 1 page <u>14</u> where an overview of the research activities conducted and not conducted is depicted.

Insights from the household survey

Internet usage, parental mediation and risky behaviour

The *Disrupting Harm* household survey in Viet Nam indicated that 89% of children aged 12–17-year-old, boys and girls alike, are internet-users – i.e., they have used the internet in the past three months. Among internet-using children, 87% use the internet every day. Most children appeared to have some knowledge of online safety skills such as knowing how to report harmful content on social media – but only 36% reported that they had received information on how to be safe online.

Although 77% of caregivers are themselves daily internet users, only 25% encouraged their children to explore and learn things on the internet, and even fewer suggested ways of using the internet safely or shared activities with their children online. Meanwhile, 19% of caregivers said that they would restrict their child's internet access if their child was bothered by something online. Most children said that their caregivers do not always allow them to go online when they want or need to (teachers also impose such restrictions).

A majority of children demonstrated some awareness of the risks in online behaviours such as meeting online acquaintances or sharing sexual images, and indeed a minority reported that they had engaged in risky behaviours online. Within the year preceding the survey, 5% had met someone face-to-face after first encountering them online – many of these encounters did not result in immediate harm and most respondents described being pleased about the outcome – while 1% reported that they had shared naked images or videos of themselves online with others.

Children's experiences of online child sexual exploitation and abuse

As part of the household survey, children were asked whether they had been subjected to OCSEA within the past year. OCSEA refers to situations that involve digital or communication technologies at some point during the continuum of abuse or exploitation. OCSEA can occur fully online or through a mix of online and in-person interactions between offenders and children.

Instances of OCSEA measured in the survey included, for example, unwanted requests to talk about sex and unwanted requests for images showing their private parts. Other examples of OCSEA captured in the survey included the proportion of children who were offered gifts in return for sexual images or who had been threatened or blackmailed to. It is encouraging to learn that most children who received the unwanted requests, offers or threats refused to do as they were asked.

The proportions of children who said that these things had happened to them varied between 0.2% and 2%, depending on the question or form of OCSEA asked about. For instance, 0.5% of surveyed children said sexual images of them had been shared without their permission in the past year and 2% of the 15–17-year-olds had accepted money or gifts in return for sexual images or videos. Overall, in the past year alone, 1% internet-users aged 12–17 in Viet Nam were victims of online sexual exploitation and abuse. This includes blackmailing, sharing their sexual images without permission, or coercing them to engage in sexual activities through promises of money or gifts. Whilst the percentage may appear small, scaled to the national population, this represents an estimated 94,000 children subjected to OCSEA in just one year¹. It is also likely that the true figures are even higher given the likelihood that children may be reluctant to speak openly about a largely sensitive subject. It was not possible to shed further light on the context around these data in the absence of qualitative research with government representatives and frontline service providers.

1. A weight was constructed to estimate the absolute number of 12–17-year-old children in Viet Nam affected by OCSEA, based on the 2019 Vietnam Population and Housing Census, specifically by obtaining population totals by age. Note that this is a crude estimate that should be interpreted as a best approximation only.

66 ·

The majority of the children in the household survey who said they had been subjected to instances of OCSEA either did not speak to anyone about the incident or confided only in their friends, and did not tell an adult, the police or a helpline.

77 ·

Compared to the other Disrupting Harm countries, these figures are surprisingly low (in four other Southeast Asian countries² where the Disrupting Harm survey was conducted, the rates ranged from 2% to 13%). It is possible that OCSEA is less common in Viet Nam, but the research team suppose the result is much more likely to indicate that children did not feel comfortable to disclose that they had experienced these things to the survey administrators due to strong social norms discouraging discussion of sex, and/or privacy concerns. This is a plausible explanation given that the CyberTips for Viet Nam from the U.S. National Center for Missing and Exploited Children (NCMEC) were at consistent rates with the other Southeast Asian countries, suggesting the problem is similarly present in Viet Nam. Unfortunately, without the possibility to conduct the qualitative research activities such as interviews with government representatives, interviews with young people and surveys of frontline social support workers, it is difficult to interpret this trend fully.

The proportion of children who said sexual images of them had been shared without their permission in the past year was 0.5%. Among 15–17-year-olds, 2% had accepted money or gifts in return for sexual images or videos. Once again, the percentages are low compared to the other *Disrupting Harm* countries, and it was not possible to shed further light on the context around these data in the absence of qualitative research with government representatives and frontline service providers.

Offenders of online sexual exploitation and abuse

Consistent with the evidence about 'offline' violence against children, persons already known to the child – often adults – were responsible for most instances of OCSEA referred to in the household survey. Individuals previously unknown to the child were involved less frequently. While this is a consistent finding across different experiences of OCSEA, it should nonetheless be interpreted with caution due to limited sample sizes. However, it is recommended that prevention and awarenessraising activities should not focus too heavily or exclusively - on the threat from strangers. This should also be a consideration for response systems, as it could be much more difficult for victims to seek help if they are emotionally and/or economically dependent on abusers.

Disclosure of online sexual exploitation and abuse

The majority of the children in the household survey who said they had been subjected to instances of OCSEA either did not speak to anyone about the incident or confided only in their friends, and did not tell an adult, the police or a helpline. The main reasons children gave for not disclosing were that they felt the incident was not serious enough, nothing would be done, they were worried about getting in trouble, and/or that they did not know where to go or whom to tell.

Other research and the comments of law enforcement authorities suggest that stigma, ignorance and indifference contribute to the under-reporting of child sexual abuse in Viet Nam. Fears and shame related to the strong emphasis on the importance of female virginity, family honour and community reputation in Vietnamese culture may be serious impediments to disclosure and reporting.

^{2.} Cambodia, Indonesia, Philippines, and Thailand.

Insights from crime data and written responses provided by law enforcement agencies

Law enforcement data

Official crime statistics do not specifically tag OCSEA-related crimes, making it difficult to assess the number of reported OCSEA cases. Data for all child sexual abuse and exploitation (including OCSEA) supplied by the INTERPOL National Central Bureau Hanoi show that there were 4,320 cases in the three years from 2017–2019.

NCMEC CyberTip data

There has been a high and rising trend in the number of CyberTips referencing Viet Nam made by electronic service providers to the NCMEC. This might indicate a high and growing incidence of OCSEA, particularly Child Sexual Abuse Material (CSAM) related offences. Viet Nam registered some of the largest numbers of CyberTips in the world. The country ranks 13th in the world for 2019. This suggests that estimates from the *Disrupting Harm* household survey may be low due to under-reporting.

Research using Google Trends points to strong interest in CSAM in Viet Nam, including image and video content depicting sexual activity with and between teenagers, with children and with babies.

Viet Nam is also a potential destination for travelling sex offenders. For example, the U.S. Angel Watch Center made 133 referrals to Viet Nam between 2017 and 2019 concerning travel to the country by registered sex offenders. However, none were reported to have been refused entry.

Law enforcement and court systems

There are two specialised units engaged in the investigation of child sexual exploitation and abuse, including OCSEA, in Viet Nam: the Anti-Human Trafficking Crime Section of the Criminal Investigation Police Department (CID), and the Cyber Security and Cyber Crime Department (CSCCD), which supports the CID in investigating OCSEA cases. Despite two units independently addressing different aspects of the crime area, a specialised unit with appropriate capacity building is critical to improve the overall response to OCSEA.

The Criminal Investigation Police Department's Anti-Human Trafficking Crime Section reported that its staff are fully trained in investigative practices, including child-friendly investigation skills. Training has been provided to the specialist units by international organisations and foreign law enforcement agencies. There is also strong cooperation with internet service providers and telecommunications companies, which are obliged by law to coordinate with investigators and provide information to identify Internet Protocol (IP) subscribers and users.

The findings from the law enforcement capacity assessment suggest that financial resources, the number of officers and the equipment available may all be insufficient for the investigation of OCSEA cases. No specific information was provided on child interview rooms, victim identification capacity, forensic capacity or financial investigation capacity. Viet Nam does not seem able to prevent travelling child sex offenders of which it is notified from entering the country as there is evidence that Viet Nam has not responded properly to notifications of child sex offenders entering the country.

Legal and policy analysis

Desk research identifies that some child-friendly practices are provided for in laws and written procedures. The Criminal Procedure Code (2015) and the Law on Children (2016) incorporate important safeguards to minimise re-traumatisation for victims of OCSEA during court procedures, to provide them with services and to uphold their right to compensation.

Legal analysis, on the other hand, pointed to inadequacies in the legal framework for preventing and responding to OCSEA. Online grooming, livestreaming of child sexual abuse, sexual harassment and online sexual extortion are not exhaustively or specifically criminalised in Vietnamese law. Although producing, trading and possessing with intent to distribute any type of pornography is banned, CSAM is not defined, nor specifically prohibited and appropriately penalised.

The government recently adopted its first-ever National Programme on Child Online Protection, covering the years 2021–2025. The Programme seeks: to protect information, privacy and personal secrets when children access information and participate in activities in the cyber environment; to prevent and address efforts to take advantage of the cyber environment to perpetrate prohibited acts against children; and to equip children with digital knowledge and skills, in accordance with their age, for protecting themselves and interacting safely in the cyber environment, and for reporting any cases of child abuse. This is a promising step forward.

Key insights

The report for Viet Nam concludes by highlighting four key insights from the research:

- 1. A large majority of children in Viet Nam have access to the internet, and most of these children go online every day. This is also the case for caregivers. However, only about one third of children have received some form of online safety training.
- 2. Internet-using children in Viet Nam are already being subjected to OCSEA. The data from the household survey suggest that there is considerable awareness of OCSEA risks among children and caregivers, but disclosure, seeking help and reporting to formal mechanisms is very low.
- **3.** Law enforcement systems are in place. However, establishing a specialised unit and strengthening capacity through training could improve the overall response.
- **4.** Some child-friendly court processes are provided for in laws and policies, but important OCSEA-related legislation, policies and standards are not yet enacted in Viet Nam. Further research is needed to assess the experiences of accessing justice by victims of OCSEA.

The report ends with a set of recommendations for action based on the data described in this *Disrupting Harm in Viet Nam [SNAPSHOT]*. These recommendations point the way forward for the government, the law enforcement, justice and social services sectors and those working within them. These are too detailed to be recounted in the Executive Summary but can be found on page <u>69</u> of this report. As with all the settings in which children live and grow, the online environment may expose them to risks of sexual exploitation and abuse. Yet the scarcity of the available evidence makes it difficult to grasp the nature of the harm caused, or to advise on governments' approaches to prevention and response. Informed by the 2018 WeProtect Global Alliance Global Threat Assessment³ and a desire to understand and deepen the impact of its existing investments, the <u>Global</u> <u>Partnership to End Violence against Children</u>, through its Safe Online initiative, decided to invest in research to strengthen the evidence base – with a particular focus on 13 countries across Eastern and Southern Africa and Southeast Asia.

The countries of focus in the Southeast Asian region are: Cambodia, Indonesia, Malaysia, the Philippines, Thailand and Viet Nam. The countries of focus in the East and Southern Africa region are: Ethiopia, Kenya, Mozambique, Namibia, South Africa, Tanzania and Uganda.

In the other *Disrupting Harm* target countries, a full set of nine research activities (and a desk and legal review) were conducted, which allows for data points to be triangulated and consolidated into a full and comprehensive picture of OCSEA. However, in Viet Nam, only four research activities could be conducted:

- A nationally-representative household survey of 994 internet-using children aged 12–17-years-old and one of their caregivers;⁴
- 2. Quantitative crime case data analysis;
- **3.** Qualitative capacity assessments of law enforcement authorities; and
- 4. The collection of non-law enforcement data

Due to complex government regulations, permission to conduct the remaining *Disrupting Harm* research activities was not forthcoming nine months after the first request. It was therefore not possible to conduct a number of the research activities of the *Disrupting Harm* methodology, which would provide important contextual information. Activities not conducted were:

- **5.** Interviews with children and caregivers who had accessed the formal justice system;
- **6.** Interviews with justice professionals on access to justice for OCSEA victims;
- 7. Survey of frontline social support workers;
- **8.** Interviews with key government representatives; and
- **9.** Conversations with OCSEA survivors to provide them with a voice.

Consequently, while *Disrupting Harm in Viet Nam* [*SNAPSHOT*] offers important evidence based on the household survey data and law enforcement inputs, this report does not contain information about how the national legal and protection systems are responding to these crimes. When drawing more detailed conclusions and designing interventions tailored to the situation in Viet Nam, data from the full range of stakeholders is needed for a complete picture, in order to ensure the most effective responses.

^{3.} WeProtect Global Alliance. (2018). <u>Global Threat Assessment 2018</u>: <u>Working together to end the sexual exploitation of children online</u>. London: WeProtect Global Alliance.

^{4.} Caregivers include all adult family members providing care to the child.

Please see Figure 1 <u>page 14</u> where an overview of the research activities conducted and not conducted is depicted.

Data collection for the household survey took place in Viet Nam from November 2020 through to February 2021. Data from law enforcement agencies focused on crime data from the three-year period of 2017–2019. Analysis was finalised in August 2021.

The desired outcome of this report is to provide data and insights that can be used by policy makers in Viet Nam to tackle OCSEA, strengthen victim support and as a catalyst to collect further evidence on OCSEA in Viet Nam. Recommended actions proposed in the report are aligned with the Model National Response and contribute to the 2030 Agenda for Sustainable Development.

Summary of methods used by ECPAT in Viet Nam

Literature review and legal analysis

A literature review was undertaken to inform the research teams prior to primary data collection. Comprehensive analysis of the legislation, policy and systems addressing OCSEA in Viet Nam was conducted and finalised in June 2020. More information on the method can be found <u>here</u>, while the full report on the legal analysis can be found <u>here</u>.

Non-law enforcement data collection

A range of non-law enforcement stakeholders have data and insight on the nature and scale of OCSEA. Data were obtained from the International Association of Internet Hotlines (INHOPE), the Internet Watch Foundation (IWF) and Child Helpline International (CHI). Qualitative insight was provided by a number of global technology platforms. Where relevant, this information supplements the analysis contributed by INTERPOL (see below).

Summary of methods used by INTERPOL in Viet Nam

Quantitative case data analysis

Data was sought on cases related to OCSEA from the national law enforcement authorities via the INTERPOL National Central Bureau in Hanoi. Data for Viet Nam were also obtained from the mandated reports of U.S.-based technology companies to the National Center for Missing and Exploited Children (NCMEC), and from other foreign law enforcement agencies.

Qualitative capacity assessments

In addition to seeking data on OCSEA cases, INTERPOL requested data on the capacity of the national law enforcement authorities to respond to this type of crime. Particular emphasis was placed on human resources, access to specialist equipment and training, investigative procedures, the use of tools for international cooperation, achievements and challenges.

Unlike in other *Disrupting Harm* focus countries, INTERPOL was unable to conduct interviews directly with law enforcement officers responsible for investigating OCSEA in Viet Nam. Instead, a unique arrangement was made under which INTERPOL National Central Bureau Hanoi took responsibility for collecting the data requested by INTERPOL from specialised law enforcement units within the country. This leads to some limitations regarding the INTERPOL data and their subsequent analysis.

More information on the methods can be found <u>here</u>.

Summary of methods used by UNICEF Office of Research – Innocenti in Viet Nam

Household survey of internet using children and caregivers

In order to understand children's use of the internet as well as the risks and opportunities they face online and their specific experiences of OCSEA, a nationally representative household survey was conducted face-to-face with 994 internet-using children while adhering to COVID 19-related restrictions and procedures in force in the country at the time. The target population for the survey was children aged 12–17-years-old in Viet Nam who had used the internet in the three months before the interview. Additionally, one parent or caregiver of each child was interviewed. Consequently, 455 (46%) boys and 539 (54%) girls were surveyed. By age, 314 (32%) 12–13-year-olds, 342 (34%) 14–15-year-olds and 337 (34%) 16–17-year-olds were surveyed.

To achieve a nationally representative random sample, the survey used random probability sampling with national coverage. Fieldwork coverage was 95%; the Northwest region was not covered due to its remoteness/inaccessibility. Coverage is defined as the proportion of the total population that had a chance of being included in the survey sample – i.e., the fieldwork would cover the area where they live if sampled. Regions where data collection was conducted included: Central Highlands, Mekong River Delta/Southwest, North Central, Northeast, Red River Delta, Hanoi, Red River Delta – Other, South Central Coast and Southeast.

The sampling followed a three-stage random probability clustered sample design to select 100 primary sampling units. The primary sampling unit considered was a Commune/Ward (10,623 people). The primary sampling units list (sampling frame) was based on the Vietnam Population and Housing Census 2019 provided by the General Statistics Office. Approximately 30% of the provinces in the country were sampled from the targeted regions. The reason for including this stage for these countries was to yield a sample that was slightly more clustered, given that the fieldwork was based in the selected provinces only. **Selection of provinces:** The required number of provinces per region was allocated in proportion to the population of each region. So that more provinces were selected in regions with larger populations. Provinces were then sampled systematically in each region, with equal probability of selection. An issue with this approach is that it can mean that important national cities or provinces are left out of the sample. To ensure that this did not happen, important provinces (such as those containing capital city) were included in the sample as separate regions.

Selection of primary sampling units: The number of units to sample per selected province was allocated proportionately based on the total number of primary sampling units for the region and province. The required number units were systematically randomly sampled with probability proportional to size. This ensured that the national distribution by level of urbanity is achieved.

At the final stage, interviewers randomly selected addresses in the field using random walk procedures and attempted contact at the selected addresses to screen for members of the survey population using a screening question developed for this purpose. Individuals (children and caregivers) were selected within each eligible household using random methods.

In every household visited, *Disrupting Harm* attempted to collect data on the number of 12–17-year-old children in the household, their gender and whether they had used the internet in the past three months. This made it possible to estimate internet penetration rates for all 12–17-year-old children in Viet Nam.

The fieldwork took place between 21 November 2020 and 22 February 2021. Data collection was carried out by Ipsos MORI on behalf of UNICEF Office of Research – Innocenti.

A more detailed explanation of the methodological approach and the specific methods used for analysis of the household survey data can be found <u>here</u>.

Ethical Approval

UNICEF's protocol was reviewed and approved by the Health Media Lab (HML) Institutional Review Board. At national level, the *Disrupting Harm* project was incorporated into UNICEF Viet Nam's annual workplan, which was approved by the Ministry of Labour, Invalids and Social Affairs (MOLISA). Both INTERPOL's research activities entailed written interviews with law enforcement officers in relevant units dealing with OCSEA. The team of interviewers took an online course on <u>Responsible Conduct</u> of <u>Research from the Collaborative Institutional</u> <u>Training Initiative</u> and followed the <u>INTERPOL Code</u> <u>of Conduct</u>.

National Consultation

The first national consultation for the main findings and recommendations in this report took place on 19 October 2021, during which government and other stakeholders were asked to comment on the recommendations made in *Disrupting Harm in Viet Nam [SNAPSHOT]* with the aim of ensuring that they were relevant for the Viet Nam context. A second consultation also took place on 13th Dec 2021.

Figure 1: Disrupting Harm methods in Viet Nam.



Legal analysis

ABOUT ONLINE CHILD SEXUAL EXPLOITATION AND ABUSE

Child sexual abuse refers to various sexual activities perpetrated against children (persons under 18), regardless of whether the children are aware that what is happening to them is neither normal nor acceptable. It can be committed by adults or peers and usually involves an individual or group taking advantage of an imbalance of power. It can be committed without explicit force, with offenders frequently using authority, power, manipulation or deception.⁵

Child sexual exploitation involves the same abusive actions. However, an additional element of a threat or of an exchange for something (e.g., money, shelter, material goods, immaterial things like protection or a relationship), or even the mere promise of such, must also be present.⁶

Online child sexual exploitation and abuse (OCSEA) refers to situations involving *digital, internet* and *communication technologies* at some point during the continuum of abuse or exploitation. OCSEA can occur fully online or through a mix of online and in-person interactions between offenders and children.

Disrupting Harm focuses on how technology can be mis-used to facilitate child sexual exploitation and abuse. Its use of the term OCSEA does not refer to abuse or exploitation that occurs exclusively online, nor is it the intention of *Disrupting Harm* to create an artificial divide between online and offline child sexual exploitation and abuse. Children can be abused or exploited while they spend time in the digital environment, but equally, offenders can use digital technology to facilitate their actions, e.g., to document and share images of in -person abuse and exploitation or to groom children to meet them in person. *Disrupting Harm* also focuses on how technology facilitates child sexual exploitation and abuse and contributes evidence needed to understand the role digital technology plays in perpetrating sexual violence against children.

Any characterisation of OCSEA must recognise that the boundaries between online and offline behaviour and actions are increasingly blurred⁷ and that responses need to consider the whole spectrum of activities in which digital technologies may play a part. This characterisation is particularly important to keep in mind as children increasingly see their online and offline worlds as entwined and simultaneous.⁸

For *Disrupting Harm*, OCSEA was defined specifically to include child sexual exploitation and abuse that involves:

- Production, possession or sharing of child sexual abuse material (CSAM): Photos, videos, audios or other recordings, or any other representation of real or digitally generated child sexual abuse or sexual parts of a child for primarily sexual purposes.⁹
- Live-streaming of child sexual abuse: Child sexual abuse that is perpetrated and viewed simultaneously in real-time via communication tools, video conferencing tools and/or chat applications. In most cases, the offender requesting the abuse in exchange for payment or other material benefits is physically in a different location from the child(ren) and the facilitators of the abuse.

^{5.} Interagency Working Group on Sexual Exploitation of Children. (2016). <u>Terminology Guidelines for the Protection of Children from Sexual</u> <u>Exploitation and Sexual Abuse</u>. Bangkok: ECPAT International. 18.

^{6.} Interagency Working Group on Sexual Exploitation of Children. (2016). <u>Terminology Guidelines for the Protection of Children from Sexual</u> <u>Exploitation and Sexual Abuse</u>. Bangkok: ECPAT International. 24.

^{7.} May-Chahal, C., & Palmer, C. (2018). <u>Rapid Evidence Assessment: Characteristics and vulnerabilities of victims of online-facilitated child sexual</u> <u>abuse and exploitation</u>. Independent Inquiry into Child Sexual Abuse. UK: Lancaster University.

Stoilova, M., Livingstone, S., Khazbak, R. (2021). <u>Investigating Risks and Opportunities for Children in a Digital World: A rapid review of the</u> <u>evidence on children's internet use and outcomes</u>. *Innocenti Discussion Papers* no. 2021-01, Florence: UNICEF Office of Research – Innocenti.
 Interagency Working Group on Sexual Exploitation of Children. (2016). <u>Terminology Guidelines for the Protection of Children from Sexual</u> <u>Exploitation and Sexual Abuse</u>. Bangkok: ECPAT International. 40.

• Online grooming of children for sexual purposes: Engagement with a child via technology with the intent of sexually abusing or exploiting the child. While international legal instruments¹⁰ criminalising grooming indicate that this must take place with intent to meet the child in person, it has become increasingly common for offenders to sexually abuse children by, for example, manipulating them into self-generating and sharing CSAM through digital technologies, without necessarily having the intention of meeting them and abusing them in person.

Besides these main concepts, the *Disrupting Harm* reports also address other phenomena that contribute to understanding the contexts and sociocultural environments in which OCSEA occurs.

The sharing of self-generated sexual content involving children¹¹ can lead to or be part of OCSEA, even if this content is initially produced and shared voluntarily between peers, as it can be passed on without permission or obtained through deception or coercion. **Sexual extortion of children**¹² refers to the use of blackmail or threats to extract sexual content or other benefits (e.g., money) from the child, often using sexual content of the child that has previously been obtained as leverage.

Sexual harassment of a child¹³ and **unwanted exposure of a child to sexual content**¹⁴ are other phenomena which can represent or enable OCSEA. For example, offenders can deliberately expose children to sexual content as part of grooming to desensitise them to sexual acts. However, for the purposes of evidence-based policy and programme development, it is important to acknowledge that there are differences between voluntary viewing of sexual content by children and viewing that is forced or coerced. The former is not included in the definition of OCSEA used in the *Disrupting Harm* study.

10. The only two legally binding international instruments containing an obligation to criminalise the grooming of children for sexual purposes are: Council of Europe. (2007). <u>Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse. Council of Europe Treaty Series –</u> <u>No. 201</u>. Article 23; and European Parliament and Council. (2011). <u>Directive 2011/92/EU on combating the sexual abuse and sexual exploitation of</u> <u>children and child pornography, and replacing Council Framework Decision 2004/68/JHA</u>. Article 6.

11. Cooper, K., Quayle, E., Jonsson, L. & Svedin, C.G. (2016). Adolescents and self-taken sexual images: A review of the literature. Computers in Human Behavior, vol. 55, 706–716.

12. Interagency Working Group on Sexual Exploitation of Children. (2016). <u>Terminology Guidelines for the Protection of Children from Sexual</u> <u>Exploitation and Sexual Abuse</u>. Bangkok: ECPAT International. 52.

13. Interagency Working Group on Sexual Exploitation of Children. (2016). <u>Terminology Guidelines for the Protection of Children from Sexual</u> Exploitation and Sexual Abuse. Bangkok: ECPAT International. 21.

14. Interagency Working Group on Sexual Exploitation of Children. (2016). <u>Terminology Guidelines for the Protection of Children from Sexual</u> <u>Exploitation and Sexual Abuse</u>. Bangkok: ECPAT International. 44. Figure 2: Framing the main forms of online child sexual exploitation and abuse explored by *Disrupting Harm*.





ABOUT VIET NAM – DEMOGRAPHICS AND INTERNET USAGE

Despite increasing connectivity around the world, few countries regularly update their formal internet use statistics or disaggregate them for their child populations. This presents a challenge in understanding how young people's lives are impacted by digital technologies, particularly in low- and middle-income countries. The infographic below summarises the latest data on internet access and social media use in Viet Nam, some of which was gathered directly through the *Disrupting Harm* nationally representative household survey of internet-using 12–17-year-olds. The available data presented here provide an important backdrop for understanding the various facets of children's internet use. However, methodological limitations may affect the quality of data from secondary sources. Relying on purposive or other non-probability sampling techniques means that the data cannot be considered representative of the population in question. In other cases, variations in data collection methods and definitions of internet use pose a challenge for cross-country comparisons.



15. United Nations Population Division. (n.d.). World Population Prospects 2019.

- 16. General Statistics Office of Viet Nam. (2019). Completed Results of the 2019 Viet Nam Population and Housing Census.
- 17. United Nations Population Division. (n.d.). World Population Prospects 2019.
- 18. United Nations Population Division. (n.d.). World Population Prospects 2019
- 19. UNICEF. (2021). The State of the World's Children 2021. UNICEF, New York.
- 20. United Nations Population Division. (n.d.). World Urbanization Prospects: The 2018 Revision.
- 21. United Nations Population Division. (n.d.). <u>World Population Prospects 2019</u>
- 22. United Nations Population Division. (n.d.). World Population Prospects 2019.

ABOUT VIET NAM - DEMOGRAPHICS AND INTERNET USAGE



23. World Bank. (2020). GDP per capita (current US\$) - Viet Nam.

24. World Bank. (n.d.). Poverty & Equity Data Portal.

25. Socialist Republic of Viet Nam. (2013). The Constitution of the Socialist Republic of Viet Nam, Article 5.3.

26. International Telecommunications Union. (2020). Country ICT data: Percentage of Individuals Using the Internet.



.....



FREQUENCY OF INTERNET USE AMONG **CAREGIVERS OF INTERNET-USING CHILDREN**



n = 994 caregivers of internet-using children.

ABOUT VIET NAM - DEMOGRAPHICS AND INTERNET USAGE



27. GSM Association (2019). Mobile Economic Impact Vietnam.

28. International Telecommunication Union. (2017). ICT Development Index 2017.

29. The Global Cybersecurity Index measures the commitment of countries to cybersecurity based on the implementation of legal instruments and the level of technical and organisational measures taken to reinforce international cooperation and cybersecurity.

30. International Telecommunication Union. (2019). Global Cybersecurity Index (GCI) 2018.

Legislation related to online child sexual exploitation and abuse is limited in Viet Nam, with only a few provisions related to child sexual abuse material included in the Criminal Code,³¹ the Law on Children,³² and the more recent Cyber Information Security Law.³³

The Criminal Code effectively prohibits all pornography in general – which technically also implies the criminalisation of child sexual abuse material (CSAM). It criminalises a series of forms of conduct, including the production, duplication, publishing, transportation, trade and possession of books, magazines, pictures, films, music or other items that contain pornographic contents of any kind for distribution. All of this would cover material depicting children as well as adults.³⁴ However, a definition of CSAM is lacking. Thus, neither the Criminal Code nor any other Vietnamese law affords any special protection to children against production of CSAM, and the penalties are not commensurate with CSAMrelated crimes. Contrary to pornography in general, CSAM represent an act of sexual abuse against a child and therefore require specific legislation and appropriate penalties.

The Law on Children includes the use of children in CSAM in its definition of child sexual abuse.³⁵ However, this law too fails to provide any definition of CSAM. The Law prohibits "providing internet and other services; producing, reproducing, releasing, operating, disseminating, possessing, transporting, storing and trading in publications, toys, games and other products whose contents cause adverse influence on children's healthy development".³⁶ This provision is vague and ambiguous as it uses the term 'adverse influence' without defining the acts that constitute or amount to it.

The Criminal Code makes it an offence for any person aged 18 or over to persuade, entice or force a child under 16 to participate in a pornographic performance or watch a pornographic performance.³⁷ According to a 2019 resolution by the Justice Council of the Supreme People's Court,³⁸ this provision includes pornographic performances which are livestreamed online. However, this prohibition does not afford protection for 16–17-year-old children.

There are no specifically tailored provisions in any Vietnamese law prohibiting **online grooming** for sexual purposes or **sexual extortion** committed in the online environment. Some related acts may be penalised as other types of related crimes, e.g., the act of live-streaming may fall under the "employment of a person under 16 for pornographic purposes" as per article 147 of the Penal Code, but specific legislation to address these crimes is missing.

31. Socialist Republic of Viet Nam. (2015). Criminal Code Law No. 100/2015/QH13 (as amended by Amendment Law No. 12/2017/QH14 of 2017).

32. Socialist Republic of Viet Nam. (2016). Law on Children No. 102/2016/QH13.

33. Socialist Republic of Viet Nam. (2018). Cyber Information Security Law No. 24/2018 / QH14.

34. Socialist Republic of Viet Nam. (2015). Criminal Code Law No. 100/2015/QH13 (as amended by Amendment Law No. 12/2017/QH14 of 2017), Article 326(1).

35. Socialist Republic of Viet Nam. (2016). Law on Children No. 102/2016/QH13, Article 4(8).

36. Socialist Republic of Viet Nam. (2016). Law on Children No. 102/2016/QH13, Article 6(10).

37. Socialist Republic of Viet Nam. (2015). Criminal Code Law No. 100/2015/QH13 (as amended by Amendment Law No. 12/2017/QH14 of 2017), Article 147.

38. Justice Council of the Supreme People's Court. (2019). <u>Resolution No. 06/2019/NQ-HDTP guiding the application of a number of provisions of</u> <u>Articles 141, 142, 143, 144, 145, 146 and 147 of the Penal Code & the adjudication of sexual abuse cases with persons under 18 as victims</u>. Article 3. The Cyber Information Security Law, which came into effect on 1 January 2019, includes provisions for ensuring the cybersecurity of children. In particular, the law makes agencies, organisations, caregivers, teachers, child carers and other relevant individuals responsible for guaranteeing children's rights and protecting children in accordance with the Law on Children when they use the internet, including protecting children from coming into contact with pornographic products. ³⁹ Although the Cyber Information Security Law does not criminalise OCSEA per se, it is still relevant as part of the legal framework to protect children from OCSEA.

Under the Criminal Code, engaging in sexual intercourse or other sexual activities with a person under the age of 13 is deemed rape (statutory rape).⁴⁰ Furthermore, the Criminal Code makes it an offence to use violence or the threat of violence, or to take advantage of a victim's defencelessness or employ other devious means, "to engage in non-consensual sexual intercourse or other sexual activities' with persons between 13–16 years of age."⁴¹ Persons between 14–16 years of age bear criminal responsibility for rape and for the rape of a person under 16 years of age.⁴² If the criminal conduct related to CSAM referred to in the Criminal Code is **committed outside Viet Nam** by a citizen, corporate legal entity of Viet Nam or stateless resident of Viet Nam, it is punishable in Viet Nam as if the offence had been committed in Viet Nam.⁴³ The Criminal Code also stipulates that extraterritorial jurisdiction would apply if the offence is committed **against a citizen of Viet Nam**.⁴⁴

In June 2021 the Government of Viet Nam approved the first-ever **National Programme on Child Online Protection** for 2021–2025. The programme aims to protect children from violence, exploitation and abuse on the internet and support safe and healthy online interactions.⁴⁵ It commits the government to developing laws, policies, practices and products that can help children harness digital opportunities and protect them from harm. Moreover, the government will work hand in hand with the internet and communication technology industry to keep up with the pace of change, protect children from new risks and harms to which they may be exposed and ensure that the internet stays safe for children.

39. Socialist Republic of Viet Nam. (2018). Cyber Information Security Law No. 24/2018 / QH14, Article 29(4).

^{40.} Socialist Republic of Viet Nam. (2015). <u>Criminal Code Law No. 100/2015/QH13</u> (as amended by <u>Amendment Law No. 12/2017/QH14</u> of 2017), Article 142(1)(b).

^{41.} Socialist Republic of Viet Nam. (2015). <u>Criminal Code Law No. 100/2015/QH13</u> (as amended by <u>Amendment Law No. 12/2017/QH14</u> of 2017), Article 142(1)(a).

^{42.} Socialist Republic of Viet Nam. (2015). <u>Criminal Code Law No. 100/2015/QH13</u> (as amended by <u>Amendment Law No. 12/2017/QH14</u> of 2017), Article 12(2).

^{43.} Socialist Republic of Viet Nam. (2015). <u>Criminal Code Law No. 100/2015/QH13</u> (as amended by <u>Amendment Law No. 12/2017/QH14</u> of 2017), Article 6(1).

^{44.} Socialist Republic of Viet Nam. (2015). Criminal Code Law No. 100/2015/QH13 (as amended by Amendment Law No. 12/2017/QH14 of 2017), Article 6(2).

^{45.} UNICEF. (2021, June 11). UNICEF Congratulates Viet Nam for Launching its First Programme on Child Online Protection [Press release].

Viet Nam is a member of the Association of South East Asian Nations (ASEAN) and as such, in October 2021 committed to the endorsed Regional Plan of Action for the Protection of Children from All Forms of Online Exploitation and Abuse in ASEAN⁴⁶ which includes commitments for member states to strengthen online child protection in the region. The plan includes seven focus areas ranging from awareness raising, strengthening data collection, to legislative reform. Also relevant is the ASEAN Regional Plan of Action on the Elimination of Violence against Children (2016-2025). Furthermore, in 2019, Viet Nam adopted the Declaration on the Protection of Children from all Forms of Online Exploitation and Abuse in ASEAN. Through agreement to these regional commitments, Viet Nam has shown dedication to address sexual exploitation of children. A more detailed ASEAN Regional Plan of Action on OCSEA has been launched on 14 February 2022, which holds specific recommendations on addressing this crime. This regional commitment is a rich resource to improve child protection standards and policies on OCSEA, enhance the capabilities of professionals, establish a unit specialised in investigating OCSEA-related crimes, strengthen data collection mechanisms, raise awareness on the issue and engage with the private sector to combat these crimes.47

In June 2021 the Government of Viet Nam approved the firstever National Programme on Child Online Protection for 2021– 2025. The programme aims to protect children from violence, exploitation and abuse on the internet and support safe and healthy online interactions.



1. CHILDREN ONLINE IN VIET NAM

The main focus of this report is to present the perspectives of young people around the exploitation and abuse of children facilitated or committed through digital technologies. However, it is important to situate these offences within the wider context of children's internet use in Viet Nam. This first chapter therefore presents a brief overview of data from the household survey about children's internet access and the activities enjoyed by children online, before going on to describe the occurrence of riskier online activities and the ways in which these are perceived by children and caregivers.

1.1.1 Internet access and use

Data from the *Disrupting Harm* household survey of children (n = 1416) suggest that 89% of 12–17-year-old children in Viet Nam are connected to the internet – i.e., they have used the internet within the past three months.^{48, 49} This figure rises from 82% among children aged 12–13 to 93% among children aged 14–15 and to 97% among children aged 16–17. No gender difference was observed in access to internet. In rural areas, 88% of children were internet users compared to 93% in urban areas, which is a relatively minor difference.

Almost all internet-using children in Viet Nam go online on a regular basis. From the household survey, 89% reported to go online on a daily basis. As in other countries around the world,⁵⁰ older children are more frequent users. No gender difference was found in relation to frequency of internet use (see Figure 3).

All surveyed children reported using the internet at home – another common trend globally.^{51,52} In addition, 75% of the children had gone online at school and 71% in internet cafés, and 55% reported having used the internet at a mall – typically less than once a month.



Figure 3: Frequency of children's internet use.

48. While conducting the random walk to identify eligible children to partake in the main survey, *Disrupting Harm* also collected data from every household visited about the number of 12–17-year-old children living there, their gender, age, and whether they had used the internet in the past three months. This allowed for an estimation of internet penetration rates for all 12–17-year-old children in Viet Nam. n = 1,416 households.
49. The question used to determine whether a 12–17-year-old was an internet user was: "Has [PERSON] used the internet in the last three months? This could include using a mobile phone, tablet or computer to send or receive messages, use apps like Facebook, WhatsApp, Instagram, send emails, browse, chat with friends and family, upload or download files, or anything else that you usually do on the internet.".
50. See Global Kids Online: http://globalkidsonline.net/.

51. Smahel, D., Machackova, H., et al. (2020). <u>EU Kids Online 2020: Survey results from 19 countries</u>. Florence: UNICEF Office of Research – Innocenti. 52. Kardefelt Winther, D., Livingstone, S., & Saeed, M. (2019). <u>Growing up in a connected world</u>. Innocenti Research Report. Florence: UNICEF Office of Research – Innocenti. As in most other countries, smartphones were by far the most popular devices used by 12–17-year-olds to go online, likely due to their relatively low cost and portability.⁵³ Nearly all (98%) internet-using children in this age group in Viet Nam used smartphones to go online, while only 21% used computers and 5% used tablets. Use of computers was more common among the older children aged 16–17, boys and children living in urban areas. Among children that used mobile phones to go online, 61% shared it with someone else – most likely to a parent (36%) than siblings (7%) or friends (1%). More younger children aged 12–13 (63%) shared mobile phones compared to the older 16–17-year-olds (16%). No gender difference was found in mobile phone sharing.

1.1.2 Caregiver internet use

Most (77%) of the caregivers in the household survey used the internet every day and only 11% have never used it. There is no notable difference by gender for caregivers' frequency of internet use. However, fewer caregivers aged 50 and above used the internet, compared to younger caregivers (see Figure 4).

As many caregivers have experience of using the internet – and children generally use the internet at home – caregivers in Viet Nam could play an important role in guiding their children's use. The smaller number of caregivers who have limited online experience might need further support and knowledge to be able to guide their children's use. Schools, too, may be able to further support caregivers in protecting their children online by including guidance on online safety and OCSEA in their curricula. However, a prerequisite to ensuring this is done effectively is that teachers receive adequate training.

1.1.3 Barriers to internet access and use

Overall, 74% of the surveyed internet-using children faced barriers in accessing and using the internet. Restriction from caregivers is the most common barrier to internet access and use for internet-using



Figure 4: Frequency of caregiver's internet use.

53. Kardefelt Winther, D., Livingstone, S., & Saeed, M. (2019). Growing up in a connected world. Innocenti Research Report. Florence: UNICEF Office of Research – Innocenti.



Figure 5: Barriers to access for internet-using children.

Base: Internet-using children aged 12-17 in Viet Nam. n = 994.

children in Viet Nam. Over half of the children in the survey, boys and girls alike, said they were unable to go online when they wanted or needed to because caregivers did not allow them access. In addition, 28% of surveyed children said that caregivers often limited how much time they spent online and 52% said they did so sometimes. About one child in three (33%) was also either not allowed to visit a social networking site at all or only allowed with permission/supervision. Similar results were found for using instant messaging apps (32%), sharing photos, videos or music online with others (36%) and watching video clips (32%). Ten percent of the children said they were not allowed to play online games at all and 33% were only allowed with permission or supervision. This suggests that a considerable proportion of children in Viet Nam are restricted from accessing online opportunities as often as they would like.

Restriction from teachers is the second most common barrier to internet access and use. Over a third (36%) of the children surveyed found themselves unable to go online when they wanted or needed to because teachers did not allow them to. Boys (40%) were more likely than girls (34%) to cite restrictions from teachers as a barrier to internet access. Younger children aged 12–13-yearsold (41%) were also more likely to face restrictions from caregivers and teacher than older children aged 16–17-years-old (34%). Children in rural areas (53%) were more likely than their counterparts in urban areas (48%) to face the barrier of restriction from caregivers.

Poor internet connections and the high cost of the internet/data were the other notable barriers to internet use for children in Viet Nam, though less frequent. More older children aged 16–17-years-old than younger 12–13-year-olds were affected by poor internet connection and high data costs – probably because they are more frequent users. Girls were more likely than boys to mention poor internet connections and high data costs as barriers to internet access. Poor internet connection inhibited internet use more for children in rural areas compared to those in urban areas. Cost of the internet affected rural and urban children in nearly equal measure.

The household survey indicated that the most popular online activities for children were entertainment activities – namely, watching videos, using social media and instant messaging. Many children also said they go online for school work and to look up new information. Older children generally engage in a wider range of online activities than younger children. It is worth considering that these categories are not intended to be mutually exclusive – for example, a child could go online to watch a video as part of their school work. Nonetheless, Figure 6 below provides a greater understanding of how 12–17-year-olds in Viet Nam use the internet and the activities they enjoy.

Gender differences are relatively minor and older children are generally involved in a wider range of activities than the younger ones – as is typical in other countries.⁵⁴ Girls are slightly more likely than boys to engage in most activities – particularly, the use of instant messaging, talking to family or friends who live far away and following celebrities – while many more boys than girls play online games weekly (see Figure 6).

Online activities	Total	12-13	14–15	16–17	Воу	Girl
Watching videos	91%	85%	93%	94%	91%	91%
Using social media	88%	78%	91%	95%	85%	91%
Using instant messaging	87%	73%	93%	95%	82%	92%
School work	72%	69%	73%	75%	73%	72%
Looking for news	70%	55%	72%	83%	68%	73%
Talking to family or friends who live far away	65%	54%	70%	72%	59%	70%
Watching a live-stream	63%	58%	64%	66%	62%	64%
Following celebrities and public figures on social media	52%	45%	53%	57%	46%	57%
Searching for new information	50%	37%	50%	60%	50%	49%
Playing online games	49%	47%	47%	53%	69%	33%
Seeking emotional support	45%	40%	44%	51%	49%	42%
Looking for information about work or study opportunities	43%	41%	44%	45%	39%	47%
Participating in a site where people share their interests	36%	30%	33%	45%	35%	36%
Looking for health information	29%	19%	31%	37%	27%	31%
Looked for information or events in local neighbourhood	23%	20%	21%	28%	23%	23%
Creating their own video or music	9%	6%	9%	11%	6%	11%
Discussing political or social problems	6%	8%	6%	6%	5%	7%
Creating a blog or website	6%	7%	7%	6%	6%	7%

Figure 6: Activities children engage in online at least once a week.

Base: Internet-using children aged 12–17 in Viet Nam. n = 994 children.

54. Livingstone, S., Kardefelt Winther, D., & Saeed, M. (2019). <u>Global Kids Online Comparative Report</u>. Innocenti Research Report. Florence: UNICEF Office of Research – Innocenti.

1.3 PERCEPTIONS AND EXPERIENCES OF RISKY ONLINE ACTIVITIES

Discussion of online risks often hinges upon adult-centric perceptions. To ensure we also understand children's perceptions, they and their caregivers were asked about their engagement in, and perceptions of, various risky online activities.

1.3.1 Contact with online strangers

A common concern around children's online activities is their exposure to 'stranger danger'. When asked to rate the riskiness of various forms of online behaviour, 52% of the caregivers in the survey said that talking to someone on the internet who they have not met face-to-face before - was 'very risky' for children. However, internet-using children were much less concerned, with only 33% ranking this activity as 'very risky' for children their age (see Figure 7). While a majority of children recognised that these activities carried some level of risk, 28% of children said that speaking to online strangers was not risky at all. In actual practice, as many as 56% of the children surveyed said that they looked for new friends or contacts on the internet while 33% of children added people they had never met before to their contact lists.

1.3.2 Sharing personal information online

Among surveyed internet-using children in Viet Nam, 57% considered sending their personal information to someone they had never met face-toface 'very risky', compared to 76% of caregivers. While a majority of children recognised that this activity carried some level of risk, 8% of children found it not risky at all to share personal information with people they know only through the internet. In actual practice, 22% of the children surveyed had shared their personal information online with someone they had never met face-to-face (see Figure 8).

Figure 7: Level of risk attributed by children to speaking to someone unknown online.



Base: Internet-using children aged 12–17 in Viet Nam. n = 994

1.3 PERCEPTIONS AND EXPERIENCES OF RISKY ONLINE ACTIVITIES

Figure 8: Level of risk attributed by children to sharing their personal information with someone unknown online.



Base: Internet-using children aged 12–17 in Viet Nam. n = 994

Figure 9: Level of risk attributed by children to meeting people in person, whom they first met online.



Base: Internet-using children aged 12–17 in Viet Nam. n = 994

1.3.3 Meeting someone in-person following an online interaction

Among surveyed internet-using children in Viet Nam, 51% considered meeting someone face-to-face whom they had first got to know online was 'very risky', a perception shared by 72% of caregivers. While many children recognised that this activity carried some level of risk, 10% found it not risky at all to meet up in person with someone that they had first got to know online. In actual practice, of the children surveyed, 5% had met someone in person who they first met online (see Figure 9).

81% 80% 70% 60% 50% 40% 30% 23% 20% 9% 10% 4% 2% 2% 0% Proud Happy Anxious Don't know Excited Prefer not to say Thoughtful

Figure 10: How children felt the last time they met someone face-to-face whom they had first got to know on the internet.

Base: Children who, within the past year, have met someone face-to-face whom they first got to know on the internet. n = 53.

Out of these children, the great majority were happy about the experience (see Figure 10). Research done across more than 30 countries around the world has produced similar findings.^{55,56}

Meetings between children and people they have only previously encountered online take different forms, from one-on-one meetings with adults to connecting with new children in the community first online and then in person, or going to group events with caregivers. Research conducted in more than 30 countries around the world has shown that children can see these nuances.^{57,58} The experiences of most internet-using children in Viet Nam seem to indicate that the risk of harm from meeting someone you do not know in person for the first time is relatively low. This may simply be how young people sometimes make new friends. However, if harm occurs, it can be very severe. While many children in Viet Nam are aware that engaging with online strangers carries a level of risk, it is important to ensure that all children are informed and taught how to engage safely and responsibly. Children should not meet with online contacts in person without taking safety precautions. In a 2020 assessment on violence against women and children in Viet Nam, children reported being approached by online strangers who would ask them to talk about sex or to share naked pictures.59

^{55.} Smahel, D., Machackova, H., et al. (2020). <u>EU Kids Online 2020: Survey results from 19 countries</u>. Florence: UNICEF Office of Research – Innocenti. 56. Livingstone, S., Kardefelt Winther, D., & Saeed, M. (2019). <u>Global Kids Online Comparative Report</u>. Innocenti Research Report. Florence: UNICEF Office of Research – Innocenti.

^{57.}Livingstone, S., Kardefelt Winther, D., & Saeed, M. (2019). <u>Global Kids Online Comparative Report</u>. Innocenti Research Report. Florence: UNICEF Office of Research – Innocenti.

^{58.} Smahel, D., Machackova, H., et al. (2020). <u>EU Kids Online 2020: Survey results from 19 countries</u>. Florence: UNICEF Office of Research – Innocenti. 59. UNICEF, UN Women, UNFPA. (2020). A rapid assessment on violence against women and children (VAWC) as an impact of COVID-19 crisis and support needs for designing targeted communication activities and responses, 30.

Children's digital skills and knowledge of online safety

Although only 36% (mostly older children aged 16–17-years-old) of the children in the Disrupting Harm survey said that they had received training on how to be safe online, the majority claimed to have knowledge of online safety skills such as knowledge of online privacy settings (75%), awareness of which images to share and not to share with friends online (89%) and knowledge of how to report harmful content on social media (71%). Just over half (55%) reported knowledge of how to check if a website can be trusted. These percentages were highest among older children aged 16-17-yearsold and lowest among the younger 12–13-year-olds. Gender differences in digital skills and knowledge are minor. It is possible that Vietnamese children overestimate their digital safety skills, which appear to be largely self-taught or acquired informally. There may be a need for more comprehensive training or sensitisation on how to be safe online.

Caregivers' responses to potentially risky behaviour

Adults tend to view all unknown people online as being ill-intentioned, whereas children's immersion in online platforms encourages them to regard online strangers as new friends and contacts. For many caregivers, the natural reaction to online risks is to remove their children's devices or restrict their internet use in other ways in a bid to protect them from possible harm. When asked in the survey what they would do if their child was bothered by something online, only 19% said they would restrict their child's access to the internet. The majority (75%) of caregivers said they would talk to the child about what happened and 45% said they would seek help or advice on what to do from someone they trust (45%). The household survey with children found that a substantial proportion of children faced restrictions from caregivers on their use of the internet and only a few have caregivers who provide a supportive environment.

44

Caregivers' supportive mediation: Contrary to the above, the household survey with children found that a substantial proportion of children faced restrictions from caregivers on their use of the internet (see <u>chapter 1.1.2</u>, above), and only a few have caregivers who provide a supportive environment. The survey found that 25% children have caregivers who often encourage them to explore and learn things on the internet. Only 17% reported that caregivers often suggest ways to use the internet safely and only 12% often do shared activities with them online.

Caregivers' digital skills and knowledge: The low caregiver supportive mediation amidst high internet restriction might be attributed to the low digital skills and knowledge among the caregivers. While only 11% of the caregivers have never used the internet and 77% (among the users) use it on a daily basis, only 37% admitted that they know more about the internet than their children. Similarly, only 20% admitted to knowing how to change privacy settings and 33% reported knowledge of how to report harmful content on social media.

Caregivers and Guiding Children's Internet Use

Caregivers' awareness of online risks, and their grasp of basic digital skills, are crucial in ensuring their children are well-equipped to stay safe online. In Viet Nam, many internet-using children face restrictions on when to go online and what to do online. There is also low supportive mediation from caregivers for online activities.

Restriction from caregivers and teachers is the most common barrier to internet access and use for internet-using children in Viet Nam. This approach might reduce children's exposure to online risks in the short term, but it also reduces their digital skills and familiarity with the online environment in the long term. On the other hand, supportive engagement and mediation by adults has been associated with positive skills development for children in other countries.⁶⁰ Supportive mediation could include engaging in activities together, talking to children about their internet use, and educating them about the risks that exist online and how best to avoid them. In these ways, children can benefit from the many useful activities and skills that the internet has to offer, while being provided with parental guidance and support in case they encounter online harm. Caregivers are therefore an important line of defence in protecting children from online harms.

The survey found that few children have caregivers who often encourage them to explore and learn things on the internet, or suggest ways to use the internet safely or often do shared online activities with them. In addition, many caregivers admitted that their children know more about the internet than them. Many caregivers also reported low knowledge of online safety skills such as how to change privacy settings online, or how to report harmful content on social media.

As many caregivers have experience of using the internet – and children generally use the internet at home – caregivers in Viet Nam could play an important role in guiding their children's use. The caregivers who have limited online experience and digital skills will need further support and knowledge to be able to guide their children's use. Schools, too, may be able to further support caregivers in protecting their children online by including guidance on online safety and OCSEA in their curricula. However, a prerequisite to ensuring this is done effectively is that teachers receive adequate training as well.

60. Livingstone, S., Kardefelt Winther, D., & Saeed, M. (2019). <u>Global Kids Online Comparative Report</u>. Innocenti Research Report. Florence: UNICEF Office of Research – Innocenti.

1.3.2. Seeing sexual images online

Perceptions of risk

Over half (60%) of the children surveyed believed that seeing sexual images or videos on the internet is 'very risky'. Among caregivers, 83% considered seeing sexual images online 'very risky' for children. In addition, when asked to select their top three concerns for their children, 31% of the caregivers in the survey chose their child seeing sexual images or videos on the internet. This was the fourth most common response chosen, following worries about health, financial concerns or worries about their child being treated in a hurtful way, but ahead of a child becoming the victim of a crime (see Figure 11).

Incidence of seeing sexual images

Although it is perceived as 'very risky' by children and caregivers – and although pornography is illegal in Viet Nam – a substantial number of children are sometimes exposed to sexual images. As shown in Figure 12, of the internet-using children in the survey, 14% said that they had sometimes seen sexual images or videos online intentionally within the past year. It is possible that children under-report seeing such images intentionally because it is a sensitive and private issue. Seeing sexual images or videos intentionally online was more common among older children aged 16–17-years-old (24%) than the younger 12–13-year-olds (6%), and more common among boys (16%) than girls (12%). Separately, 23% of the children said that they had sometimes seen sexual images or videos online by accident. The children who had seen sexual images or videos online by accident came across this content most frequently on online advertisements (58%) and on social media (46%). Seeing sexual images or videos accidentally online was also more common among older children aged 16–17-years-old (36%) than the younger 12-13-year-olds (12%), but more common among girls (26%) than boys (19%).



Figure 11: Caregivers' top concerns regarding their children.

Figure 12: Level of risk attributed by children to seeing a sexual image or video on the internet.



Base: Internet-using children aged 12-17 in Viet Nam. n = 994

Seeing sexual content online is not OCSEA. However, it could be related to OCSEA. Accidental or intentional glimpses of sexual content are one thing; being exposed to sexual images as part of a grooming process intended to desensitise the child and pave the way for subsequent requests for images or sexual acts is another. While viewing violent or degrading sexual content can serve to normalise harmful gender norms and sexual behaviour, seeing some pornography appears to be an increasingly present experience for young people.⁶¹ Addressing both phenomena is needed.

Over half (60%) of the children and 83% of caregivers surveyed believed that seeing sexual images or videos on the internet is very risky for children. 23% of the children have sometimes seen sexual images or videos online by accident.

1.3.3 Making and sharing self-generated sexual content

From the household survey, 58% of the internet-using children and 61% of the caregivers believed that it is wrong for a person to take naked images or videos of themselves. In practice, 0.5% (n = 5) of the 994 children surveyed said they had taken naked pictures or videos of themselves in the past year. The true figure could be higher, as some children may have chosen not to mention such behaviour due to discomfort about discussing it or because pornography is illegal. None of the children reported allowing someone else to take naked pictures or videos of them in the past year, though 0.8% (n=8) preferred not to say.

61. See for example: Crabbe, M. & Flood, M. (2021). <u>School-Based Education to Address Pornography's Influence on Young People: A Proposed</u> <u>Practice Framework</u>. American Journal of Sexuality Education 16(1).
1.3 PERCEPTIONS AND EXPERIENCES OF RISKY ONLINE ACTIVITIES

Figure 13: Level of risk attributed by children to sending sexual content online.



Base: Internet-using children aged 12-17 in Viet Nam. n = 994

The children and caregivers in the survey also concurred that it is risky to share sexual images online. Among the children, 78% thought it 'very risky' (Figure 13). Only 5% did not find it risky at all. In practice, only 0.6% (n = 6) of the 994 surveyed internet-using children said that they had shared naked pictures or videos of themselves online in the past year. Notably, 1.5% (n=15) children preferred not to respond.

The main reasons given by the six children in the Viet Nam household survey who said they had shared sexual images or videos of themselves was because they were flirting and having fun, in love and/or they trusted the other person. Two of the six children shared the images with someone they met online who had no other connection with their life. Four shared the images with a friend or someone else they knew in person and one with a romantic partner. The percentage of children in the Viet Nam household survey who said they had shared sexual images of themselves online are lower than those seen in other *Disrupting Harm* target countries. However, as permission was not granted for some of the other planned research activities which could provide some context to these findings, *Disrupting Harm* is unable to provide possible interpretations as to why this might be.

The main reasons given by the six children in the Viet Nam household survey who said they had shared sexual images or videos of themselves was because they were flirting and having fun, in love and/or they trusted the other person.

The Global Rise in Self-generated Sexual Content involving Children

Around the world, the increasing use of technology is leading to shifts in notions of privacy and sexuality among children, particularly adolescents.⁶² Forms of behaviour that are increasingly normative to young people can be bewildering for adults who grew up in a different time. For example, chatting and video live-streaming is frequent, whether among small private groups of friends or large, anonymous public audiences. While much of this is harmless, producing and sharing self-generated sexual content using these tools is also increasing and bringing significant risks.⁶³

The sharing of self-generated sexual content by children is complex and includes a range of different experiences, risks and harms. *Disrupting Harm* data from other countries and in Viet Nam shows that some self-generated content is shared with others because children are flirting and having fun, or are in love. Such exchanges are increasingly becoming part of young people's sexual experiences. However, self-generated sexual content can be coerced from children, for example, through threats or peer pressure.

While coercion can clearly be seen as a crime and leads directly to harm, there can be negative consequences for children sharing any sexual content including in cases where sharing is not coerced. Material shared willingly may not cause harm at first, but there remain risks if it is later shared beyond the control of the person who created it. Once it exists, such content can also be obtained through deception or use of coercion and circulated by offenders perpetually (see Figure 14).^{64,65} The legal ban of pornography in Viet Nam⁶⁶ may add an extra layer of complexity to this issue. Because of the ban, victims of coerced sharing may be afraid to report their case as they could expose themselves to criminalisation for the production of such content.

Figure 14: Mapping the consequences of sharing self-generated sexual material involving young people.



Livingstone, S. & Mason, J. (2015). <u>Sexual Rights and Sexual Risks among Youth Online: A review of existing knowledge regarding children and young people's developing sexuality in relation to new media environments</u>. London: European NGO Alliance for Child Safety Online.
Thorn & Benson Strategy Group. (2020). <u>Self-Generated Child Sexual Abuse Material: Attitudes and Experiences. U.S.: Thorn.</u>
Bracket Foundation. (2019). Artificial Intelligence: <u>Combating Online Sexual Abuse of Children</u>. 10.

65. EUROPOL. (2019, 9 October). Internet <u>Organised Crime Threat Assessment 2019</u>. Netherlands: EUROPOL.

66. Socialist Republic of Viet Nam. (2015). Criminal Code Law No. 100/2015/QH13 (as amended by Amendment Law No. 12/2017/QH14 of 2017), Article 326(1).

2. ONLINE CHILD SEXUAL EXPLOITATION AND ABUSE IN VIET NAM

Following on from children's perceptions of, and participation in, various risky online practices, this chapter will turn to the threat of online child sexual exploitation and abuse in Viet Nam. *Disrupting Harm* draws on a variety of sources – including law enforcement data and mandated reports related to Viet Nam from United States-based technology companies to the National Center for Missing and Exploited Children (NCMEC) – in order to create a well-rounded presentation of the nature of these crimes against children. This chapter includes estimates of the occurrence of certain instances of OCSEA based on data from law enforcement units and children's self-reported experiences. For several reasons, these estimates are not intended to provide a conclusive picture of the prevalence of OCSEA. Firstly, the existing administrative data accessed, such as that kept by law enforcement authorities, rarely delineates or classifies OCSEA elements. Secondly, with respect to the household survey, a degree of under-reporting is to be expected due to privacy concerns and hesitation to discuss sexual activity and experiences of sexual exploitation and abuse. This appears to have been particularly common in Viet Nam, where the reported OCSEA figures are considerably lower than other countries in the region. Furthermore, in households where sexual abuse occurs, it is plausible that researchers were unlikely to get permission to speak to those children for the survey. Finally, many estimates are based on analysis of sub-samples of the survey data that are small because OCSEA is still a rarely reported phenomenon, which results in a larger margin of error.

While *Disrupting Harm* has full confidence in the data and the quality of the sample obtained, the challenges of researching specific and sensitive phenomena mean the loss of some precision in the final estimate. For these reasons, it is suggested that the reader interprets the findings in this chapter as an approximation of the occurrence of certain crimes against children related to OCSEA in Viet Nam and the extent to which internet-using children in Viet Nam are subjected to OCSEA.

Official crime statistics do not specifically tag indicators of OCSEA-related crimes.

2.1 LAW ENFORCEMENT DATA

The analysis here draws on qualitative and quantitative data from domestic and foreign law enforcement authorities in order to shed light on the offences committed in the country, the characteristics and behaviour of offenders and victims, and crime enablers and vulnerabilities. The quantitative data are reported numbers and not a complete picture of OCSEA prevalence.

2.1.1 Reported CSEA offences

Official crime statistics do not specifically tag indicators of OCSEA-related crimes. Data were obtained instead for the more general category of CSEA offences (see Figure 15) but the proportion of these crimes which were committed by means, or with the aid, of digital technology is unknown.

The data shared with INTERPOL were cumulative figures for the 2017–2019 period, so it is not possible to study trends over time. Likewise, the national data did not suffice to identify the incidence of CSEA in different locations.

Figure 15: Number of CSEA offences recorded by law enforcement authorities in Viet Nam, 2017–2019.

Offence	2017–2019
Rape against children	1,400
Forcible sexual intercourse with children	20
Sexual intercourse with children	2,100
Obscenity against children	800
Total	4,320

Base: Data supplied by INTERPOL National Central Bureau Hanoi.

This total corresponds well with an assessment ordered by the National Assembly of Viet Nam⁶⁷ on child abuse. The monitoring team reported 8,442 cases of child abuse in the period from 1 January 2015 until 30 June 2019, which included 6,432 child victims of sexual abuse.⁶⁸

2.1.2 Characteristics and patterns of OCSEArelated offending

The national law enforcement authorities provided the following information on the *modus operandi* of OCSEA offenders:

- Deserted places or private apartments were often used to abuse children.
- Offenders took advantage of the emotional vulnerability of the victims to entice them for sexual purposes.
- Economically disadvantaged sections of the population were particularly targeted.
- Offenders used materials and coercion to entice children for the purposes of sexual abuse. Grooming was used as a technique to normalise abuse and exploitation. In many grooming cases, abuse was compensated for with goods and/ or cash.
- Offenders took advantage of close relationships with the victims.
- Victims lacked information, awareness and knowledge about OCSEA, which accentuated their vulnerability.
- Social media platforms were used extensively to identify, to reach out to and to establish contact and build trust and confidence with prospective victims.

67. Socialist Republic of Viet Nam. (2019). Resolution No. 81/2019/QH14. 68. Cong an Nhan Dan Online. (2020, 27 May). <u>The number of abuse children has increased dramatically, there are seven abused children per day</u> in the country.

	2017	2018	2019	2020	% CHANGE 2017 to 2018	% CHANGE 2018 to 2019	% CHANGE 2017 to 2019	% CHANGE 2019 to 2020	% CHANGE 2017 to 2020
Viet Nam	272,286	710,037	379,555	843,963	29%	-1%	27%	137%	202%
Global Total	10,214,753	18,462,424	16,987,361	21,751,085	81%	-8%	66%	28%	113%
Viet Nam as % of Global Total	2.67%	3.85%	2.23%	3.88%					

Figure 16: Number of CyberTips concerning suspected child sexual exploitation in Viet Nam.

Base: CyberTip data supplied by NCMEC.

2.1.3 NCMEC CyberTips

United States federal law requires that U.S.based electronic service providers (i.e., technology companies) based in the United States report instances of suspected child exploitation on their platforms to CyberTips of the National Center for Missing and Exploited Children (NCMEC). NCMEC triages these reports and passes CyberTips on to the relevant countries' national law enforcement units for action. However, for providers not based in the United States, this reporting is voluntary. As not all platforms report suspected child exploitation to NCMEC, the data below do not encompass several platforms popular in the *Disrupting Harm* focus countries.

Trends in CyberTips for Viet Nam

Figure 16 shows there has been a rising trend in CyberTips concerning suspected child sexual abuse and exploitation in Viet Nam. This might indicate a high and growing incidence of OCSEA, particularly CSAM-related offences. The number of CyberTips for Viet Nam increased by 27% between 2017 and 2019. A year-on-year increase of 161% in 2018 was followed by a decline of 27% in 2019. While the year 2019 saw a decline in all CyberTips globally,⁶⁹ the decline in Viet Nam was less marked. Moreover, the data for 2020 – which has been included in the figure even though it did not form part of the study period – point to a surge in CyberTips for Viet Nam that is much steeper than the rebound in global reports.

Reports referencing Viet Nam made up 2.09% of the total number of CyberTips worldwide in 2019 – and 3.88% in 2020. This proportion has been consistently higher than in other *Disrupting Harm* countries. It is also higher than expected, given that Viet Nam accounts for just 1.25% of the world's population, and just 1.67% of the global internet-using population (see <u>About Viet Nam –</u> <u>Demographics and internet usage</u>).

CyberTips by type of incident

Analysis of CyberTips for Viet Nam reveals that the possession, manufacture and distribution of CSAM (referred to in U.S. legislation as 'child pornography') account for almost all of Viet Nam's reports in the reporting period (see Figure 17).

^{69.} The dip in the number of CyberTips in 2019 must be read and understood in the context of changes in procedures that resulted in fewer reports but an increase in the average number of files contained in each report. As part of its efforts to streamline the reporting mechanism, the NCMEC has worked closely with its industry partners to ensure that they deliver more comprehensive reports. As a result, more companies have started to include more than one file per report, rather than submitting a separate report for each and every image and multiple reports per suspect.

Figure 17: CyberTips concerning suspected child sexual exploitation in Viet Nam, by incident type.

Incident Type	2017	2018	2019
CSAM, including possession, manufacture and distribution (NCMEC classification: child pornography) ^{70,71}	272,265	710,029	379,541
Travelling child sex offences (NCMEC classification: child sex tourism) ⁷²	1	1	2
Child sexual trafficking		1	1
Child sexual molestation		2	2
Online enticement of children for sexual acts	20	3	9
Unsolicited obscene material sent to a child		1	
Total	272,286	710,037	379,55

Base: CyberTip data provided by NCMEC.

NCMEC CyberTips by electronic service provider

Almost all CyberTips for Viet Nam in 2017–2019 came from electronic service providers. A total of 50 electronic service providers submitted at least one report of suspected child exploitation for Viet Nam in this period. This suggests some diversity in the platforms used by the general population and by suspected OCSEA offenders. Data for the 20 platforms which submitted the largest numbers of reports in 2019 are shown in Figure 18.

Facebook has consistently been responsible for the great majority of CyberTips for Viet Nam, with almost 98% of the total in 2019. Although the volumes are far smaller, notable increases have been observed in reports from Google, Imgur, Instagram, Twitter, Flickr and Pinterest.

Suspensions by Twitter

Analysis conducted by Twitter for *Disrupting* Harm of approximately three million URLs shared by accounts suspended for violation of the platform's CSEA policy has found that OCSEA-related activity on the platform falls largely into two categories: the sharing of links to third-party servers on which CSAM is hosted, and users connecting to other CSAM producers. The links to third-party servers are further subdivided into URL shorteners such as bit.ly, ift.tt, dlvr.it, goo.gl, and ow.ly, and generic social media links (Instagram, YouTube, Reddit, Facebook, etc.). Together, these account for 50% of the CSAM-related links shared on Twitter. Twitter has confirmed that in the years 2017 to 2019, users in Viet Nam were suspended for suspected CSEA-related activity.

71. CyberTips under this category may reference more than one file of CSAM. For example, some reporting electronic service providers include more files per report, as opposed to one image per report and multiple reports per suspect.

72. The terminology used by NCMEC is 'Child Sex Tourism', to align with U.S. legislation. *Disrupting Harm* advocates for the use of the term 'Travelling Child Sex Offences' in line with the Luxembourg Guidelines.

^{70.} The terminology used by NCMEC is 'child pornography', to align with U.S. legislation. *Disrupting Harm* advocates for the use of the term 'child sexual abuse material' in line with the <u>Luxembourg Guidelines</u>.

2.1 LAW ENFORCEMENT DATA

Figure 18: CyberTips concerning suspected child sexual exploitation in Viet Nam, by top 20 reporting electronic service providers.

Reporting Electronic Service Provider	2017	2018	2019	% of 2019 Total
Facebook	268,175	702,976	370,401	97.59
Google	2,800	5,512	7,060	1.86
Imgur LLC	27	17	764	0.20
Instagram Inc	137	737	599	0.16
Twitter Inc/ Vine.co	92	42	176	
SnugMug Flickr		167	121	
Pinterest Inc	51	103	110	
Discord Inc			80	
Tumblr	58	114	63	
Microsoft Online Operations	75	96	51	
Adobe systems Incorporated	1	2	19	
Snapchat		2	13	
Tinder Inc		1	11	
Roblox	4	1	9	
Tagged.com	3	2	9	
Reddit Inc	1	1	7	
sendvid	10	4	6	
Yahoo Inc	197	49	6	
Dropbox Inc	11	6	5	
Multimedia LLC/Zmedianow LLC/Chaturbate	2	7	5	

Base: CyberTip data supplied by NCMEC, sorted by 2019 counts, null results removed.73

The data for Viet Nam are notable for the number of different image-hosting and video-sharing (including randomised video chat) providers that reported. A presence in Viet Nam of OCSEA offenders with a level of technical sophistication and specialist interest may be derived from an appearance in the data of self-avowed 'moral free file host' Motherless. com, anonymous image-based bulletin board 4chan, digital forensics research company Hacker Factor and dark web and peer-to-peer monitoring firm Tiversa. The emergence in the data of platforms such as Discord and Twitch, which are often used to facilitate gaming chat and streaming, may reflect Viet Nam's adoption of tools and apps requiring greater bandwidth. Reports from skout.com, Tagged. com, Tinder and Match point to the misuse of adult dating sites for suspected distribution of CSAM. Reports from Chaturbate, a platform specialising in the provision of adult live-streamed sexual activity, which is often paid for in tokens, raise the possibility of OCSEA with a commercial element.

73. Data for reports from YouTube in 2019 appear to be lacking for all 14 focus countries. It is unclear whether this reflects zero suspected OCSEA events on the platform in that year, or whether YouTube events are included in the 2019 total for parent company Google.

Figure 19: CyberTips concerning suspected child sexual exploitation in Viet Nam – number of unique upload IP addresses by year.

	2017	2018	2019	% Change 2017 to 2019	% Change 2018 to 2019
Viet Nam Unique Upload IP Addresses	182,409	286,082	287,760	58%	1%
Total Viet Nam Reports	272,286	710,037	379,555	39%	-47%
Reports per Unique IP Address	1.49	2.48	1.32	-12%	-47%

Base: CyberTip data provided by NCMEC.

CyberTips by IP addresses

CyberTip data permits analysis of the number of unique Internet Protocol (IP) addresses used to engage in suspected child exploitation in Viet Nam (see Figure 19).

An IP address is assigned to each individual device on a specific network at a specific time.⁷⁴ Multiple reports per IP address can indicate that suspects (or at least their devices) are engaged in multiple offences of CSAM distribution during the same online session, itself perhaps also indicative of a more deliberate style of offending that is less likely to be committed through lack of knowledge. By the same token, Viet Nam's consistently low average number of reports per IP address may be suggestive of a tendency towards lower volume CSAM offending within individual online sessions on globally popular platforms.

2.1.4 Other OCSEA Threat Data

Distribution on peer-to-peer (P2P) networks

Data on CSAM distribution on peer-to-peer filesharing networks presents a rather different picture. Data captured by the Child Rescue Coalition's Child Protection System reveals that 925 Vietnamese IP addresses were identified as engaged in distribution or downloading. Since the system does not monitor all file sharing networks, this should not be taken to be representative of the sum total of CSAM offending on such platforms. By way of comparison, Figure 20 provides data for Viet Nam and other *Disrupting Harm* focus countries in Southeast Asia.

Figure 20: CSAM distribution and downloading from *Disrupting Harm* focus countries, observed on peer-to-peer file sharing networks by the Child Rescue Coalition.

	IP Addresses	Globally Unique Identifiers (GUIDs) ⁷⁵
Cambodia	1,319	95
Indonesia	1,124	202
Malaysia	2,754	558
Philippines	1,971	1,446
Thailand	3,049	609
Viet Nam	925	141

Base: Data provided by Child Rescue Coalition for the period 9 June 2019 to 8 June 2020

In some respects, distribution on peer-to-peer networks is less of an 'entry level' activity than distribution on mainstream social media platforms. While these networks are not as secured as dark net services, users are required to download specialist software and to actively upload and search for CSAM, often by filenames shared in offender networks.

74. Note that the same IP address may be counted in more than one year, and a report can contain more than one unique IP address. Technical measures by internet service providers, including the dynamic assignment of IP addresses and the sharing of IP version 4 addresses across a large number of devices, can also have an impact on the number of unique IP addresses logged.

75. A Globally Unique Identifier (GUID) is a 128-bit number created by the Windows operating system or another Windows application to uniquely identify specific components, hardware, software, files, user accounts, database entries and other items.

While fewer devices were captured sharing CSAM on the peer-to-peer networks monitored in Viet Nam than in other *Disrupting Harm* focus countries in Southeast Asia, the capture of multiple IP addresses per installation of filesharing software, represented by the number of globally unique identifiers in the above figure, indicates that the average Vietnamese offender has engaged in multiple sessions of CSAM distribution in the period sampled. These observations point to more persistent OCSEA-related offending by some individuals based in Viet Nam.

Reports from foreign law enforcement agencies

During the course of INTERPOL's research activities for Disrupting Harm, one foreign law enforcement agency reported that they had referred a total of 129 OCSEA cases to Vietnamese authorities in the period 2017–2019.76 Referrals from foreign law enforcement agencies are most often made when an ongoing investigation is found to involve an offender or victim in the second country, or when a domestic service provider makes a report to the national law enforcement authority that is indicative of OCSEA in the second country. Since data were not systematically collected concerning OCSEA referrals from all law enforcement agencies outside Viet Nam, it is likely that there were additional international referrals in the reporting period.

Web searches for CSAM

Research was conducted on Google Trends⁷⁷ with a purpose of identifying levels of interest in CSAM as revealed by open web searches. In the first instance, a sample of 20 terms selected by the INTERPOL Crimes Against Children team served as keywords and phrases for specialist interest in CSAM. Queries for the time period 1 January 2017 to 31 December 2019 on searches in Viet Nam returned a result of 'not enough data' for 16 of these 20 terms. For the remaining four terms, it was not possible to determine that the Google users were searching exclusively for CSAM.

Returns of 'not enough data' equate with a relative popularity score of zero, indicating a comparatively low level of interest in that term (rather than no search results at all) within the geographical and time limits set.⁷⁸ When compared to the results of global searches for the same terms, and to searches made in other countries in the same time frame, this suggests that specialist CSAM search terms may be used less in Viet Nam than they are in some other countries.

While it may also be argued that more sophisticated CSAM searchers are less likely to search on the open web, the relative popularity of some of the terms in the INTERPOL sample in other countries would suggest that open web searches are still used for CSAM discovery.

Less specialist, more 'entry level' searches related to CSEA were common across the country in the reporting period, including English language searches for image and video content depicting sexual activity with and between teenagers, with children and with babies. There was a particular interest in Japanese CSAM content, and terms related to *anime* and *hentai* cartoon-style images and videos were popular. Searches for CSAM-related content in particular formats, such as 'high-definition video' and '1080p', and on specific platforms, such as Tumblr, TikTok, the storytelling website Wattpad and the Singapore-based live-streaming service Bigo Live, appear to indicate that some web searchers in Viet Nam have requirements reflective of a more persistent and active interest in CSAM that has progressed beyond initial curiosity. Related searches for content on the Deep Web and for individual images and videos by file name also suggest that some Vietnamese offenders are engaged in more sophisticated CSAM offending and networking.

^{76.} INTERPOL requested data and qualitative insights from a number of foreign law enforcement agencies with intelligence on or outreach activities in the focus countries. In line with intelligence handling protocols and data protection requirements, some of these sources have been anonymised.

^{77.} Google Trends (trends.google.com) is a publicly available tool that returns results on the popularity of search terms and strings relative to others within set parameters. Rather than displaying total search volumes, the tool calculates a score (on a range of 1 to 100) for relative popularity based on the ratio of searches using the selected term or string to the total number of searches using all terms/strings within the geographical and time parameters set. For more information on data and scoring, see: FAQ about Google Trends data.

Google trend analysis suggests that CSEA-related keywords are most frequently issued in searches in Ho Chi Min, Hanoi and Da Nang, where Japanese words with sexual connotations are also used as search terms. However, this may be related to the high-speed internet connections and high levels of internet penetration in these cities. A direct correlation with the interest of people in these areas in CSAM should not be inferred.

Travelling sex offenders

Through the Angel Watch Center, U.S. Homeland Security Investigation monitors convicted sex offenders and sends referrals to countries when a registered offender travels to the respective destination country. In 2017, 30 referrals were sent to Viet Nam, 53 in 2018 and 50 in 2019. None of them were denied entry to Viet Nam. Reports made by the Angel Watch Centre of Homeland Security Investigations (HSI) were not actioned. This speaks to possible lack of coordination between specialised units and the border management authority.

Among the CyberTips described above, a small number of reports concern suspected offline incidents. These reports may reflect Viet Nam's status as a tourist destination of particular interest to travelling sex offenders. In its additional internal classification ('Incident Type 2'), NCMEC tagged 17 reports in the reporting period as related to online enticement of children pre-travel.

Previous research indicates that the consolidation of policies and law enforcement efforts to combat the sexual exploitation of children in travel and tourism in Thailand and the Philippines has purportedly diverted exploiters to Viet Nam.⁷⁹

79. Scelles, F., & Charpenel, Y. (2016). Prostitutions – exploitations, persecution, repression (4th Global Report ed.). ECONOMICA.

2.2 CHILDREN'S EXPERIENCES OF ONLINE CHILD SEXUAL EXPLOITATION AND ABUSE IN VIET NAM

Under the *Disrupting Harm* project, OCSEA is defined specifically to include CSAM, live-streaming of child sexual abuse and online grooming of children for sexual purposes. These concepts are used here to organise and present the relevant data from the Viet Nam household survey on instances of potential and actual OCSEA. However, it should be borne in mind that these experiences or offences are not completely distinct, but may occur in combination or in sequence. Moreover, online and offline sexual exploitation and abuse may also be combined, with digital technology used to facilitate or record in-person abuse.

The numbers reported in this chapter are low compared to other *Disrupting Harm* countries⁸⁰ in the region. This is likely due to under-reporting because of strong social norms discouraging discussions about sex, discomfort when it is raised, as well as concerns given the criminalisation of all forms of pornography in the country. However, it is hard to determine the reasons for under-reporting, because *Disrupting Harm* was unable to conduct five out of the nine planned research activities, some of which would have allowed for a further interpretation of these findings and provide a more comprehensive picture of the issue in Viet Nam.

This *Disrupting Harm* household survey of 12–17-yearold internet users considered various manifestations of OCSEA, which will be presented individually below. When taken together, the data suggest that in the past year alone, 1% of internet-using children aged 12–17 in Viet Nam were victims of grave instances of online sexual exploitation and abuse. This aggregate statistic encompassed four indicators including children being blackmailed to engage in sexual activities, someone else sharing their sexual images without permission, or being coerced to engage in sexual activities through promises of money or gifts in the past year prior to data collection.

According to *Disrupting Harm* estimates, when scaled to the population internet-using children in this age group in Viet Nam this represents an estimated 94,000 children who were subjected to any of these harms in the span of just one year⁸¹. It is worth considering that the survey only included internet users and those who live at home, meaning that more vulnerable child populations – such as children engaged in migration or children in street situations – were not represented in these figures.

2.2.1 Online grooming

Disrupting Harm defines online grooming as engaging a child via technology with the intent of sexually abusing or exploiting the child. This may happen either completely online or via a combination of online and in-person modalities.

Online grooming is a complex process which is often fluid and difficult to detect, especially where it involves a slow build of trust between the offender and the child over an extended period of time. The child is often 'prepared' for sexual abuse and made to engage in sexual acts online or in person by means of deceit, coercion or threats. However, the process can also be abrupt, with an offender suddenly requesting or pressuring a child to share sexual content or to engage in sexual acts. To explore multiple forms of grooming, the household survey questions included conversations about sex, requests for naked images and face-to-face meetings with the intent to engage in sexual activity.

At the time of writing, Vietnamese law does not specifically criminalise online grooming with the intent of sexually exploiting the child either online (through, for example, the production of child sexual abuse material) or offline (in person).

80. Cambodia, Indonesia, Philippines and Thailand.

^{81.} A weight was constructed to estimate the absolute number of 12–17-year-old children in Viet Nam affected by OCSEA, based on the 2019 Vietnam Population and Housing Census, specifically by obtaining population totals by age. Note that this is a crude estimate that should be interpreted as a best approximation only.

Potential grooming - children asked to talk about sex



Base: Internet-using children aged 12-17 in Viet Nam. n = 994.

In the household survey of internet-using children in Viet Nam children were asked if they were subjected to certain behaviours in the past year that could be an indication of grooming. Those children who had experienced possible instances of grooming were then asked follow-up questions about the last time this happened to them: how they felt, whether it occurred online or offline (or both), who did it to them, and whether they told anyone about it. Because relatively few children said they were subjected to possible grooming, many of these follow-up questions involve small subsamples. In such cases, when the sample is smaller than 50, absolute numbers are presented instead of percentages to avoid misinterpretation of the data. Recognising that sexual exploitation and abuse of children can happen in many different ways and places, most data points below allow for multiple responses and may add up to over 100%.

According to the household survey with 994 internetusing children in Viet Nam, 19 children (1.9%) had received unwanted requests to talk about sex or sexual acts within the past year. These were mostly older children (16–17 years), with no difference by gender. Seventeen of the 994 surveyed children (1.7%) preferred not to respond. Among the 19 children that received unwanted requests to talk about sex or sexual acts, half of them received the most recent request face-to-face, and half online via social media on Facebook (including Messenger). In the sample, five of the eight children who received unwanted requests to talk about sex online said the requests did not affect them in any way while the other three felt annoyed. Offenders and Disclosure: The unwanted requests which the eight children received online to talk about sex came about equally from persons they didn't know and from friends or acquaintances, including romantic partners. Just over half of the (5 of 8) children who received these unwanted requests online did not tell anyone about this experience. The most common reasons given by the five children who did not tell anyone were that they did not think the incident serious enough to report and the feeling that they had done something wrong. Among those children who told someone about their experience, most told someone they knew, like a sibling, caregiver or friend – rather than use formal reporting mechanisms such as social workers or a helpline.

Potential grooming – children asked to share naked images and videos



Base: Internet-using children aged 12-17 in Viet Nam. n = 994.

Of the 994 internet-using children in Viet Nam who took part in the survey, five children (0.5%) had received an unwanted request for a photo or video showing their private parts within the past year. All were girls aged 12–13 and refused to comply with the request. Fifteen children (1.5%) preferred not to respond. Among the five children that received an unwanted request for a photo or video showing their private parts, two said the request had come via social media –most commonly on Facebook. One said it had been made face-to-face and the other preferred not to say where it happened. While one of the five girls said she was not affected by the request, the others felt embarrassed, annoyed or angry. **Offenders and disclosure:** The five children received the unwanted requests to share their sexual images from different sources, including someone unknown to them, an adult friend, and a friend that was also a child. Two of the five children that received unwanted requests to share sexual images or videos of themselves told a female caregiver or a sibling. One child didn't tell anyone because she did not want the person concerned to get into trouble.

Offering children money or gifts for sexual images or videos

Only two (0.2%) of the 994 children who participated in the Viet Nam household survey said they had been offered money or gifts in return for sexual images or videos in the past year. Seven children (0.7%) preferred not to respond. The two children that had been offered money or gifts in return for sexual images or videos were aged 12–13-years-old and were girls. One offer was made in person, the other online. One of the children told a caregiver; the other preferred not to say who they had disclosed to. Of the two children that had been offered money or gifts in return for sexual images or videos, in one case the offender was an adult friend; and the other child preferred not to say who it was.

Offering children money or gifts for sexual acts

Only three (0.3%) of the 994 children in the survey – one girl from each of the three age groups – said they had been offered money or gifts to meet someone in person to do something sexual within the past year. Five children (0.5%) preferred not to respond. Two of the requests were made online via Facebook and during an online game. The offender was either an adult friend or someone unknown to child. One of the two children disclosed the incident to a caregiver and the other preferred not to say who she confided in.

Sexual extortion (Threats or blackmail to engage in sexual activities)

Sexual extortion is sometimes used in the grooming process. An offender can sometimes use previously obtained sexual images of the child to threaten him or her into sharing more images or engaging in other kinds of sexual activities. In Viet Nam, threats and blackmail to engage in sexual activities committed online is not specifically criminalised by law. Only three (0.3%) of the 994 internet-using children surveyed said that they had been threatened or blackmailed to engage in sexual activities at least once in the past year. Eight children (0.8%) preferred not to respond. None of the three children that had been threatened or blackmailed to engage in sexual activities responded to the question of whether this happened in person or online. Of the three, one said they didn't know who the offender was and the other two preferred not to say. One child told either their caregivers or a helpline; two opted not to say who they disclosed the incident to.

2.2.2 CSAM and live-streaming of child sexual abuse

As seen in the <u>Overview of Legislation and Policy</u> at the beginning of this report, the Vietnamese Criminal Code does not clearly criminalise CSAM, although provisions on pornography in general could potentially be used to prosecute CSAM-related offences. Although the Criminal Code does not explicitly criminalise the live-streaming of sexual abuse of children all ages, the Justice Council of the Supreme People's Court indicated that the provision which makes it criminal to persuade, entice or force a child under 16 to participate in a pornographic performance or watch a pornographic performance,⁸² also refers to performances live-streamed online.⁸³

^{82.} Socialist Republic of Viet Nam. (2015). Criminal Code Law No. 100/2015/QH13 (as amended by Amendment Law No. 12/2017/QH14 of 2017), Article 147.

^{83.} Justice Council of the Supreme People's Court. (2019). Resolution No. 06/2019/NQ-HDTP guiding the application of a number of provisions of Articles 141, 142, 143, 144, 145, 146 and 147 of the Penal Code & the adjudication of sexual abuse cases with persons under 18 as victims . Article 3.

CSAM reporting

As shown in Figure 20, Viet Nam has been identified as a hosting country for images and videos assessed as illegal by the member hotlines of International Association of Internet Hotlines (INHOPE) contributing to the ICCAM platform.⁸⁴

Figure 21: CSAM hosting in Viet Nam, as identified by International Association of Internet Hotlines (INHOPE) members' hotlines using ICCAM.

Victim Age Group	2017	2018	2019
Illegal items (confirmed CSAM)	11	5	10
Percentage of global total	0.01%	0.00%	0.00%

Base: Data provided by INHOPE.

However, data pertaining to the ICCAM project are limited to submissions from INHOPE member hotlines, while the Internet Watch Foundation operates primarily as the United Kingdom's CSAM hotline. Consequently, the figures do not represent the sum total of CSAM hosting in the country.

The Internet Watch Foundation responded to seven reports concerning confirmed CSAM hosting in Viet Nam in 2017 and three in 2019.

Children subjected to non-consensual sharing of sexual images



Base: Internet-using children aged 12-17 in Viet Nam. n = 994.

In the household survey, five (0.5%) of the 994 internet-using children aged 12–17-years-old in Viet Nam declared that someone had shared sexual images of them without their permission. These images, and particularly those shared online, can be widely circulated and viewed repeatedly all over the world, resulting in a continuous sense of shame and fear of being recognised. When these images or videos are recordings of severe sexual abuse, the trauma associated with those in-person experiences can also be repeatedly reactivated by the sharing of the content. Fifteen children (1.5%) preferred not to respond to this question.

Offenders and Disclosure: Of the five children in the survey sexual images of whom had been shared without their permission, three said the offender was someone unknown to them. Two of the five children preferred not to disclose who the offender was. The non-consensual sharing of sexual images occurred online, via social media platforms – particularly Facebook and Instagram. Three of the five children did not disclose what had happened to anyone. They said that this was because they were worried that they would get in trouble if they told someone, or because they feared it would cause trouble for them or their family. One child that disclosed, confided in a friend and the other preferred not to say who they had disclosed the incident to.

The findings of the household survey show a varying perception among children and caregivers about sharing sexual images of other persons without their permission. As many as 63% of the children and 22% of their caregivers agreed that it should be illegal for a person to share images or videos of someone else naked. However, 58% of children and 57% of caregivers also attached blame to the victims in cases where they produced naked images or videos of themselves.

84. For more information on the ICCAM project, see: International Association of Internet Hotlines: What is ICCAM and Why is it Important?.

Accepting money or gifts in exchange for sexual images or videos

As explored in the context of grooming, children are sometimes offered money or gifts in return for sexual content. Here, the focus is on children accepting money or gifts in return for sexual content, regardless of how the process was initiated.

While the sexual exploitation of children is not new in Viet Nam,⁸⁵ the use of digital technologies – including by children and young people – to self-produce and send images or videos of oneself in return for money or other material incentives is an emerging trend globally. This practice could increase the risk of nonconsensual sharing: 90% of the 'youth-generated' sexual images and videos assessed in a study by the Internet Watch Foundation (IWF) and Microsoft were 'harvested' from the original upload location and redistributed on third party websites.⁸⁶ When children create sexual content in exchange for something, this constitutes child sexual exploitation, regardless of whether or not they are coerced. In Viet Nam, where all sexual content – including sexual content involving adults – is illegal, children exploited in this way could at the same time be accused of a criminal offence.

Given the sensitivity of this topic, only the 15-17year-old respondents in the household survey were asked whether they had accepted money or gifts in exchange for sexual images or videos of themselves. The household survey showed that nine (1.8%) of the 510 internet-using children in this age group had accepted money or gifts in exchange for sexual images or videos in the past year. These children were all aged 14–15-years-old years and boys. Four children (0.8%) preferred not to respond. Gaps still remain concerning this form of OCSEA. Understanding the intricacies around children's motivations to engage in this practice, their understanding of the risks involved, and how they are first introduced to this practice are important questions that require further study.

85. ECPAT International. (2018). ECPAT Country Overview Viet Nam, 7.

86. Internet Watch Foundation & Microsoft. (2015). Emerging Patterns and Trends Report #1 Online-Produced Sexual Content.

2.3 OTHER EXPERIENCES OF CHILDREN THAT MAY BE LINKED TO OCSEA

Additional to the examples of OCSEA already presented, children may be subject to other experiences online which can be harmful, such as sexual harassment or unwanted exposure to sexualised content. Moreover, these experiences could, in some instances, contribute to the desensitisation of children so that they become more likely to engage in sexual talk or sexual acts - for example, during a grooming process.

__

In the Viet Nam household survey, children reported these experiences more commonly than the forms of OCSEA presented in chapter 2.2, which was also the case in other Disrupting Harm countries.

2.3.1 Sexual Harassment



Base: Internet-using children aged 12-17 in Viet Nam. n = 994.

In the household survey, 8% of internet-using children in Viet Nam (82 children) said they had been subject to sexual comments about them that made them feel uncomfortable - including jokes, stories or comments about the child's body, appearance or sexual activities. There were no clear gender or age differences. Sexual harassment was more likely to occur in person (45%) than online (29%). Where the comments were made online, they mainly came via social media, particularly Facebook (including Messenger), with TikTok a distant second.

Offenders and Disclosure: When the 82 children who had been subject to this kind of sexual harassment in the past year were asked who was responsible, most pointed to people they already knew, such as a peer (39%) or an adult friend (16%). One child in four said the offender was someone unknown to them. While many of the 82 children that experienced this kind of sexual harassment disclosed it to someone, a large proportion (43%) did not disclose to anyone - mostly because they did not think anything would be done about it.

Children that told someone about the experience were more inclined to disclose to people they already knew, rather than through formal reporting mechanisms such as social workers or a helpline. These were most likely to be friends. It is worth noting that Vietnamese legislation does not criminalise sexual harassment.

When children who had been subject to sexual harassment in the past year were asked who was responsible, most pointed to people they already knew, such as a peer or an adult friend.

2.3.2 Receiving unwanted sexual images



Base: Internet-using children aged 12-17 in Viet Nam. n = 994.

Of the 994 children in the household survey, 52 (5%) had been sent unwanted sexual images in the past year. There were no clear gender or age differences. Most (61%) children said that they received unwanted sexual images online on social media, and fewer in person (17%). This is unsurprising as the act of sending images is clearly easier using digital technology. Once again, the most common platform where this occurred was Facebook, followed by Zalo.

Among the 52 children who had been sent unwanted sexual images, around 40% said it was done by someone unknown to them, while another 40% said it was done by someone already known; such as an adult friend or family member. One in five preferred not to say who sent the images. Of the 52 children, around half did not tell anyone the last time this happened to them. Among those that told someone, children were more inclined to tell their friends and caregivers – rather than use formal reporting mechanisms such as social workers or a helpline.

3. RESPONDING TO ONLINE CHILD SEXUAL EXPLOITATION AND ABUSE IN VIET NAM

This chapter presents the limited data *Disrupting Harm* was able to gather about current Vietnamese response mechanisms. Data are drawn from the household survey with children and from written inputs provided by the police to INTERPOL.

3.1 FORMAL REPORTING MECHANISMS

The *Disrupting Harm* team was unable to collect the full set of data as in other *Disrupting Harm* focus countries and thus neither interviews with children and caregivers who had accessed justice, nor interviews with justice professionals took place. Therefore, triangulation and interpretation of the information presented in this section is limited.

All in all, a comparison of the available law enforcement data (see <u>chapter 2.1</u>) with the data from the household survey of children suggests that a low proportion of OCSEA cases in Viet Nam are investigated and that non-reporting by children and adults is common.

3.1.1. Disclosure by children

The *Disrupting Harm* household survey data show that some children in Viet Nam are subjected to OCSEA. However, as seen in <u>chapters 2.2</u> and <u>2.3</u>, children that have, or may have, been subjected to OCSEA typically do not tell anyone what happened or only tell a friend. Specifically, most of the children who experienced unwanted requests for sexual conversation or images, who were subjected to sexual harassment or whose private images were shared without their permission did not talk to anyone.

The explanations that the children most commonly gave for their reluctance to disclose were:

- 1. That they felt the incident was not serious enough or that nothing would be done.
- 2. That they were worried about getting in trouble.
- **3.** That they did not know where to go or whom to tell.

Hardly any children used a formal reporting mechanism by talking to the police or a hot/helpline and most did not tell their caregivers.

3.1.2 Disclosure by caregivers and others

Responses from caregivers to the household survey also indicated a reluctance to report OCSEA formally. A third (33%) of caregivers said that they would tell the police if their child was subjected to OCSEA, 13% that they would call a helpline and 11% that they would tell a social welfare officer. The majority (69%) said they would talk to their spouse and 28% that they would tell a teacher at the child's school. Only 6% said they would keep it to themselves.

Others said they would not report due to concern about negative consequences, fear of not being treated properly, repercussions and/or a belief that reporting would have no effect.

On paper, two laws arguably make it a legal requirement to report cases of OCSEA to the police, although they do not specifically mention OCSEA. *The Law on Children* obliges individuals, families, agencies and organisations to report incidents of child sexual abuse.⁸⁷ The *Cyber Information Security Law* makes individuals, agencies and organisations responsible for reporting promptly to the competent agency in the event of cybersecurity threats and any cybersecurity intrusion/infringement.⁸⁸

87. Socialist Republic of Viet Nam. (2016). <u>Law on Children No. 102/2016/QH13</u>, Article 51(1).

88. Socialist Republic of Viet Nam. (2018). Cyber Information Security Law No. 24/2018 / QH14, Article 42(2).

Stigma and Under-Reporting

It has been suggested that there is stigma, ignorance and indifference around child sexual abuse-reporting in Viet Nam.⁸⁹ Under-reporting makes it difficult to understand the scale of the problem, which in turn inhibits calls for adequate prevention and intervention programmes.

There is the stigma of victimisation that stems from strong emphases on the importance of female virginity, family honour and community reputation in Vietnamese society. Collectivist values are strong, with the cohesion and reputation of family and community holding significant value.⁹⁰ Victims of rape are at risk of being blamed.⁹¹ Boys who have been sexually abused or exploited may be fearful and embarrassed to talk about it with their families.⁹² That may also be influenced by the fact that boys fear to be branded as gay – homosexuality is considered socially unacceptable in Vietnamese society and often perceived as a 'disease'.⁹³ When providing information for *Disrupting Harm*, the Criminal Investigation Department Anti-Human Trafficking Crime Section confirmed that anxiety, shame, fear of disclosing personal information, mockery and adverse public opinion based on the aforementioned aspects of Vietnamese culture could prevent women or children from reporting sexual abuse. The Cyber Security and Cyber Crime Department agreed that cultural barriers and social biases are among the factors that lead to the improper recognition of child abuse offences. Many victims and their families still do not dare to report the crime due to shame or fear of public judgments.

Officials in the Cyber Crime Department added that sexual abuse offenses cause serious physical and emotional harm to children and can even lead to the death of the victim, including by suicide. They added that most of the offenders are relatives or acquaintances of the victim. *Disrupting Harm* data across countries confirms that offenders are generally known to victims.

Children that have, or may have, been subjected to OCSEA typically do not tell anyone what happened, or only tell a friend – if they do.

^{89.} Tran, N. K., Alink, L. R. A., van Berkel, S. R., & van IJzendoorn, M. H. (2016). <u>Child Maltreatment in Vietnam: Prevalence and Cross-Cultural</u> <u>Comparison</u>. Journal of Aggression, Maltreatment & Trauma, 26(3), 211–230.

^{90.} Tran, N. K., Alink, L. R. A., van Berkel, S. R., & van IJzendoorn, M. H. (2016). <u>Child Maltreatment in Vietnam: Prevalence and Cross-Cultural</u> <u>Comparison</u>. Journal of Aggression, Maltreatment & Trauma, 26(3), 211–230.

^{91.} UNICEF Viet Nam, UNICEF Office of Research – Innocenti & University of Edinburgh (2016). Understanding The Drivers of Violence Affecting Children in Viet Nam.

^{92.} Government of Viet Nam & United Nations Viet Nam. (2012). Exploratory research – Trafficking in Boys in Viet Nam.

^{93.} World Vision Australia. (2014). Sex, Abuse and Childhood: A study about knowledge, attitudes and practices relating to child sexual abuse, including travel and tourism, in Cambodia, Lao PDR, Thailand and Vietnam.

3.1.3. Helplines

The Law on Children tasks the government with establishing an active national telephone exchange system for receiving and responding to information relating to child sexual abuse.94 In support of the provision, the National Committee for Children under the Ministry of Labour, Invalids and Social Affairs has established a National Call Centre for Child Protection with the objective of directly receiving and processing information, notices, risk denunciations and acts of child abuse.95 In 2017, the call centre was assigned a new child protection helpline number: No. 111.96,97 The state-run 111 helpline is free of charge, operates on a 24/7 basis and is a part of Child Helpline International. The three consulting centres are in the cities of Hanoi and Da Nang, and the province of An Giang. The helpline offers legal advice and responds to cases of child sexual abuse and trafficking.

Due to the limitation of not being able to conduct many of the planned research activities in Viet Nam, no information could be obtained by the Disrupting Harm team about the effectiveness of the centres in responding to cases of OCSEA or making referrals.⁹⁸ In 2019, the helpline received 506,957 calls and handled over 32,000 cases including 322 cases of child sexual abuse and 80 cases of child exploitation. Child Helpline Viet Nam reported to Child Helpline International that it received no contacts concerning OCSEA in 2017. It did not provide annual data submissions to Child Helpline International for 2018 and 2019.99 At the National Consultation on 13 December 2021, the helpline 111 also indicated that in 2020 the helpline started to disaggregate OCSEA data.

OCSEA related cases can also be reported to the Viet Nam Computer Emergency Response Team.

^{94.} Socialist Republic of Viet Nam. (2016). Law on Children No. 102/2016/QH13, Article 51(3).

^{95.} National Child Helpline. (n.d.). Introduction to the national PBX protecting children.

^{96.} Saigoneer. (2017, 8 December). Vietnam hopes to combat child abuse with new national child protection hotline at 111. Saigoneer.

^{97.} Helpline 111 is called "hotline 111" in Vietnamese, but functions more like a helpline.

^{98.} Vietnam Association for Protection of Child's Rights & ECPAT International. (2019). Sexual Exploitation of Children in Viet Nam Submission to the Human Rights Council.

^{99.} Data submissions confirmed by Child Helpline International (CHI), November 2020.

Disrupting Harm was unable to gather information on the law enforcement response to OCSEA cases in Viet Nam through interviews and surveys with relevant public officials, representatives of international and non-government organisations, victims of OCSEA (and their caregivers) or any other persons who have experienced the law enforcement response at first hand. The following information is therefore based only on written information provided to INTERPOL by key law enforcement units in response to questionnaires and has not been cross-compared with any other data sources.

3.2.1 Organisational structure and resources

There are two specialised units engaged in the investigation of child sexual exploitation and abuse, including OCSEA, in Viet Nam:

- 1. The Anti-Human Trafficking Crime Section of the Criminal Investigation Police Department, responsible for investigating crimes against children. Investigating OCSEA is one of the functions assigned to the unit.
- 2. The Cyber Security and Cyber Crime Department, which supports the Criminal Investigation Police Department in investigating OCSEA cases. The Department has merged with the High-Tech Police Department, which was mandated to conduct initial investigations of OCSEA-related crimes.¹⁰⁰

The Criminal Investigation Police Department Anti-Human Trafficking Crime Section has 30–40 permanent officers, but it is unclear whether any are working on child sexual exploitation and abuse or OCSEA cases. The Criminal Investigation Police Department Anti-Human Trafficking Crime Section reported that it has been supplied with sufficient equipment for handling OCSEA cases but shares the equipment with other units. The equipment was not specifically reported to include any forensic tool or specialist OCSEA software. Moreover, OCSEA investigations are conducted using the same internet connection as for other work assignments. With respect to the Cyber Security and Cyber Crime Department, no information was made available on the number of officers assigned to OCSEA. The Cyber Security and Cyber Crime Department lacks tools for detecting OCSEA and has insufficient equipment for conducting investigations.

In relation to financial expenses, both units reported that their operational resources are met from the national budget and are limited.

The equipment and resources currently available to the authorities for combatting OCSEA may well be insufficient, given the scale and complexity of the offences. The number of officers in the Criminal Investigation Police Department Anti-Human Trafficking Crime Section appears to be low, in comparison to the workload.

3.2.2 Investigative capability

The Criminal Investigation Police Department Anti-Human Trafficking Crime Section reports that its staff are fully trained in investigative practices, the handling of cases and child-friendly investigation skills, and that they conduct initial investigations as prescribed by law, strictly following the victimcentred approach. However, the Section did not provide any information on child-friendly interview facilities. The Section also reports that it collaborates with non-government organisations for the welfare of victims. Child-friendly communication models are understood to have been set up, and training courses on child-friendly investigations conducted, with support from UNICEF.

100. ECPAT International. (2017). Regional Overview: The Sexual Exploitation of Children in Southeast Asia.

No information was provided on specialised capacity for OCSEA such as victim identification capacity, forensic capacity or financial investigation.

Capacity for combatting travelling child sex offenders is understood to include:

- National system to monitor convicted sex offenders released from prisons in Viet Nam (however, no details were shared with *Disrupting Harm*);
- Mechanism for vetting foreign nationals with criminal records entering Viet Nam, as notified by the foreign affairs authorities, with a view to adopting appropriate measures (in its response to the questionnaire, the Criminal Investigation Police Department Anti-Human Trafficking Crime Section emphasised the importance of alerts from other countries); and
- Capacity to handle cases in other languages, with the cost of notarised translations being met from the national budget where required.

Nevertheless, foreign law enforcement data indicate that notifications sent to Viet Nam did not lead to the travellers being denied access or entry to Viet Nam (see <u>Chapter 2</u>).

The Cyber Security and Cyber Crime Department reports that its capacity for open-source investigation such as social media platforms and internet search engines is reasonably up to date. No mention was made of other OCSEA investigative capacity or capacity for victim identification, or the support needed in these respects.

3.2.3 Training and development

The Criminal Investigation Police Department Anti-Human Trafficking Crime Section regularly organises in-house training courses, study tours and workshops. Training has also been provided by foreign law enforcement agencies, the UN Office on Drugs and Crime, the International Center for Missing and Exploited Children and other such relevant organisations.

Viet Nam's Ministry of Public Security has also collaborated with the Australian Federal Police in fighting transnational serious and organised crime. In partnership with the Royal Melbourne Institute of Technology University (Hanoi), they have jointly managed and coordinated the Asia Region Law Enforcement Management Programme over the past 15 years, running programmes for over 1,000 law enforcement officials from 38 countries, including regional training programmes on child sexual exploitation. In 2019, Viet Nam hosted the 40th Asia Region Law Enforcement Management Programme, with the theme of Transnational Child Sexual Exploitation.

Despite these training and development activities, a need for investigative capacity building appears to persist. The Criminal Investigation Police Department Anti-Human Trafficking Crime Section reports a high demand for training including courses in information technology and the collection of electronic evidence, and for knowledge exchange with other countries.

Cooperation and Data Access

According to the Criminal Investigation Police Department Anti-Human Trafficking Crime Section, criminal records and case data are uploaded for access by competent authorities. Viet Nam needs to be re-connected to the INTERPOL International Children Sexual Exploitation (ICSE) database followed by a refresher training on victim identification and use of ICSE. The Criminal Investigation Police Department, the main unit dealing with this type of crime, reports that they do not have access to any INTERPOL tools. This implies that the INTERPOL International Children Sexual Exploitation Database connection has been lost. A dialogue is currently underway to reinstall the connection and train a new batch of users.

Written responses to the *Disrupting Harm* team reported that there is a regular practice of information-sharing under the Ministry of Public Security. Cooperation with other sectors is centralised, so that to engage in cooperation at either the domestic or international level, both governmental agencies and non-government organisations are required to secure permission. This could delay efforts to receive support from international law enforcement authorities and organisations.

While some law enforcement agencies under *Disrupting Harm* research countries face difficulties in cooperating with internet service providers, Viet Nam law enforcement authorities and the Criminal Investigation Police Department regularly coordinate with internet service providers and telecommunications companies, especially at the stage of evidence collection and investigation. These companies are obliged by law¹⁰¹ to coordinate with investigators and to provide information related to acquired IP address data to identify IP subscribers and users. This cooperation provides Viet Nam with a strong basis for enforcing legislation on OCSEA-related crimes.

^{101.} As per the Penal code (amended), the Children Law 2016, Law on information technology and Law on Cyber information security providers and users of Internet services are responsible for ensuring information safety and information security within their information system; cooperating with competent authorities, other organizations and individuals in ensuring online information safety and information security. Measures for ensuring online information safety and information security must be regularly taken and complied with technical regulations and standards of information safety and the laws on telecommunications and Internet service quality. Hogan Lovells. (March 6, 2019). <u>Vietnam quick to enforce new cybersecurity law</u>.

3.3 GOING TO COURT AND ACCESSING SERVICES

The *Disrupting Harm* project was unable to assess the experiences of victims of OCSEA in accessing justice through the formal court system and in obtaining services. Selected information from the desk review is provided below, but none of this information has been verified through interviews with victims of OCSEA, justice professionals or other government representatives.

3.3.1 Court procedures and compensation

The criminal justice framework of Viet Nam incorporates important safeguards to minimise re-traumatisation for victims of OCSEA during court procedures, to provide them with services and to uphold their right to compensation.

- In terms of child-friendly interview methods, the Criminal Procedure Code allows the courts to hear cases in closed session in order to protect children.¹⁰² Chapter XXVIII of the Code deals exclusively with the procedures to be followed in legal proceedings for persons under 18.¹⁰³ According to the Code, the legal proceedings must be conducted in a manner that is congenial and conformable to the age, maturity level, and awareness of these persons¹⁰⁴ and that the questioning of child defendants, victims and witnesses must be in accordance with their age and level of development.¹⁰⁵ Those presiding over such proceedings should be specially trained and experienced in dealing with children.¹⁰⁶
- Although the Criminal Procedure Code does not provide for children to access psychological support during the legal proceedings, it requires the trial panel of the court of first instance to include a teacher or youth union official, or a person with experience and psychological knowledge of children.¹⁰⁷ The Law on Children also provides that the judges, people's jurors and procurators who institute legal proceedings in cases involving children should be trained in children's rights and psychology and educational science.¹⁰⁸
- The Code entitles children to legal assistance¹⁰⁹ and the right to participate in legal proceedings through representatives such as schools, youth unions or individuals with experience and a knowledge of psychology and social affairs.¹¹⁰ Additionally, the Law on Children provides children with the right to legal aid, to state their opinions and to protection from illegal deprivation of their right to freedom. The Legal Aid Law adopted in 2017 gives concrete form to these rights by guaranteeing legal aid to all children under 16 and to child offenders and child victims aged 16–18-years-old who are in financial difficulty.¹¹¹

102. Socialist Republic of Viet Nam. (2015). Criminal Procedure Code Law No. 101/2015/QH13, Article 25; also Article 423(2).

103. Socialist Republic of Viet Nam. (2015). Criminal Procedure Code Law No. 101/2015/QH13, Article 413.

104. Socialist Republic of Viet Nam. (2015). Criminal Procedure Code Law No. 101/2015/QH13, Article 414(1)

105. Socialist Republic of Viet Nam. (2015). Criminal Procedure Code Law No. 101/2015/QH13, Article 423(4).

108. Socialist Republic of Viet Nam. (2016). Law on Children No. 102/2016/QH13, Article 81(5).

109. Socialist Republic of Viet Nam. (2015). Criminal Procedure Code Law No. 101/2015/QH13, Article 414(5).

111. ASEAN (2019). Ending Violence Against Children in ASEAN Member States. Mid-term review of priority areas under the ASEAN Regional Plan of Action on the Elimination of Violence against Children 2016–2025.

^{106.} Socialist Republic of Viet Nam. (2015). <u>Criminal Procedure Code Law No. 101/2015/QH13</u>, Article 415.

^{107.} Socialist Republic of Viet Nam. (2015). Criminal Procedure Code Law No. 101/2015/QH13, Article 423(1).

^{110.} Socialist Republic of Viet Nam. (2015). Criminal Procedure Code Law No. 101/2015/QH13, Article 414(3).

- There is no explicit legal duty to provide children with information related to legal proceedings in a child-friendly manner. However, the Law on Children allows non-governmental organisations to assist/support victims – including, presumably, during legal proceedings.¹¹²
- The Criminal Procedure Code also protects the privacy of child victims,¹¹³ stipulating that the "personal information of individuals below 18 years of age must be kept confidential".¹¹⁴ To protect child victims and witnesses, the Code limits their interaction with defendants when they are called to give testimony in court.¹¹⁵ The court may conduct the questioning with the help of the representatives of the child victims or witnesses.¹¹⁶
- The Criminal Procedure Code entitles victims of crimes or their legal representatives to recommend punitive measures and levels and guarantees of compensation.¹¹⁷ Under the Cybersecurity Law, if an offender causes loss and damage, they must pay compensation in accordance with the law.¹¹⁸ Child victims of OCSEA-related offences can therefore seek compensation under these two laws. They may also institute an independent civil case under the Civil Code for infringement of their personal rights such as the right to protection of honour, dignity and prestige.¹¹⁹ However, since children have limited legal capacity under the Civil Code, their legal representatives must claim for compensation or damages on their behalf.¹²⁰ Vietnamese laws do not provide for any country-managed funds through which child victims of OCSEA-related offences can seek compensation. Nor do they ensure that non-national victims of OCSEA-related offences can seek compensation from convicted perpetrators and/or through state-managed funds.

Not all victims attempt to obtain justice through the formal justice system. While interviews with young people and justice professionals were not permitted by the government, a 2014 World Vision study indicated that victims of child abuse and exploitation and offenders frequently negotiated extra-judicial payments in Viet Nam.¹²¹ However, at the National Consultation of 13 December 2021 MOLISA indicated that the situation has progressed since that study was conducted.

3.3.2. Access to services

As part of accessing justice, victims also need to be able to reach services that help with their recovery. The literature and legal reviews conducted for Disrupting Harm show that national legislation in Viet Nam affords child victims of sexual abuse, including OCSEA-related offences, a right to recovery and rehabilitation. According to the Law on Children, child protection initiatives should attach special importance, *inter alia*, to actively assisting disadvantaged children - a concept which includes victims of child sexual abuse¹²² – with functional rehabilitation and social inclusion.¹²³ The measures foreseen to assist children who have suffered abuse include psychological treatment, health care and physical and mental health rehabilitation,¹²⁴ social integration¹²⁵ and legal assistance.¹²⁶

^{112.} Socialist Republic of Viet Nam. (2016). Law on Children No. 102/2016/QH13, Article 92(3). 113. Socialist Republic of Viet Nam. (2015). Criminal Procedure Code Law No. 101/2015/QH13, Article 414(2). 114. Socialist Republic of Viet Nam. (2015). Criminal Procedure Code Law No. 101/2015/QH13, Article 414(2). 115. Socialist Republic of Viet Nam. (2015). Criminal Procedure Code Law No. 101/2015/QH13, Article 423(5). 116. Socialist Republic of Viet Nam. (2015). Criminal Procedure Code Law No. 101/2015/QH13, Article 423(5). 117. Socialist Republic of Viet Nam. (2015). Criminal Procedure Code Law No. 101/2015/QH13, Article 62(2)(g). 118. Socialist Republic of Viet Nam. (2018). Cyber Information Security Law No. 24/2018/QH14, Article 9. 119. Socialist Republic of Viet Nam. (2015). Civil Code Law No. 91/2015/QH13, Article 25; See also: Article 34. 120. Socialist Republic of Viet Nam. (2015). Civil Code Law No. 91/2015/QH13, Article 25(2). 121. World Vision Australia. (2014). Sex, Abuse and Childhood. A Study about knowledge, attitudes and practices relating to child sexual abuse, including travel and tourism, in Cambodia, Lao PDR, Thailand and Vietnam. 122. Socialist Republic of Viet Nam. (2016). Law on Children No. 102/2016/QH13, Article 47(6). 123. Socialist Republic of Viet Nam. (2016). Law on Children No. 102/2016/QH13, Article 47(6). 124. Socialist Republic of Viet Nam. (2016). Law on Children No. 102/2016/QH13, Article 50(2)(a). 125. Socialist Republic of Viet Nam. (2016). Law on Children No. 102/2016/QH13, Article 50(2)(d). 126. Socialist Republic of Viet Nam. (2016). Law on Children No. 102/2016/QH13, Article 50(2)(h).

At the National Consultation of 13 December 2021, Helpline 111 noted that since the disaggregation of data on OCSEA in 2020, there has been an increase in help seeking by victims of OCSEA from 186 cases in 2020 to 405 cases in 2021. Counselling centres are emerging in some Vietnamese provinces.¹²⁷ Provincial level social work centres, child advisory offices at the district level and community and school advisory points are being created by the government across the country. The centres are meant to provide counselling services to children and families, including services for children who are at risk of, or have experienced, any form of abuse or exploitation. The distribution and effectiveness of these services has not yet been evaluated.¹²⁸

Another noteworthy initiative is the free, online chat-based consulting services on sexual and reproductive health operated by the Center for Creative Initiatives in Health Population. Tens of thousands of young people have accessed the platform to gain information. The service is available through the website and Facebook page and via Yahoo Messenger.¹²⁹ 66

The criminal justice framework of Viet Nam incorporates important safeguards to minimise retraumatisation for victims of OCSEA during court procedures, to provide them with services and to uphold their right to compensation. The *Disrupting Harm* project was unable to assess the experiences of OCSEA victms in accessing justice through the formal justice system and in obtaining services.

^{127.} ECPAT International, Plan International, Save the Children, UNICEF and World Vision. (2014). <u>National Child Protection Systems in the East Asia</u> and Pacific Region: A review and analysis of mappings and assessments. Bangkok: ECPAT International.

^{128.} UNICEF Viet Nam, UNICEF Office of Research – Innocenti & University of Edinburgh (2016). Understanding The Drivers of Violence Affecting Children in Viet Nam.

^{129.} Center for Creative Initiatives in Health and Population. (n.d.). Counselling Services for Teens.

3.4.1 Policy and government

National strategies and coordination

The National Programme of Action for Children (2021–2030) contains relevant provisions regarding child-friendly justice and the prevention of violence and sexual abuse against children. More specific is the first-ever National Programme on Child Online Protection recently adopted by the government for the years 2021–2025.¹³⁰ The programme refers to online sexual abuse and voices the government's intention of addressing the legal gap with respect to the criminalisation of CSAM as well as establishing a national CSAM database.

In 2021, the Minister of Information and Communications established a Multi-agency and Interdisciplinary Network to Protect and Rescue Children in the Online Environment.¹³¹ The network coordinates the work of 24 agencies, organisations and businesses to support the Minister of Information and Communications in preventing and combating online child abuse, contributing to increased social awareness and creating a safe and healthy online environment for children. The network has the tasks of promoting communication, contributing to greater social awareness about child protection activities, receiving reports and collecting information about acts of abuse against children, and synthesising, classifying and coordinating the efforts of its members to handle complaints and information about acts of child abuse in the online environment. The network will also advise and propose policies and regulations on child protection in the online environment to competent state agencies.

In 2019, the UN Office on Drugs and Crime supported the Ministry of Public Security and the Supreme People's Procuracy in developing a set of professional guidelines for police and procurators on handling child sexual abuse cases.¹³² *Disrupting Harm* was unable to verify whether these guidelines are being used by police or prosecutors.

In 2019, the Ministry of Education and Training made classes on the prevention of sexual abuse mandatory in elementary schools. Manuals were provided. A lifeskills training programme encompassing the issue of child abuse was developed with UNICEF, and the teaching of the programme was made a condition of Child-Friendly School accreditation.¹³³ Currently the Ministry is integrating digital skills into the curriculum for students at each grade level.¹³⁴

Child protection system

The Ministry of Labour, Invalids and Social Affairs, which is the lead agency on child protection,¹³⁵ oversees the cooperation between state agencies responsible for child protection at all levels.¹³⁶ The government has established Child Protection Committees in 5,500 communes (about half of the country's communes) to cooperate with Network of Village Collaborators.¹³⁷

Despite improvements in the policy and legal framework for child protection, Viet Nam's child protection system remains underdeveloped and overly reliant on – especially at grassroots level – untrained and overloaded social welfare officers. There is not only a lack of trained Child Protection Officers at district and commune levels,¹³⁸ but also a lack of clear procedures in cases of child abuse. Overlaps between agencies and lack of knowledge of laws and procedures are persistent problems.¹³⁹

 Ministry of Public Security of Socialist Republic Of Viet Nam. (2019, 20 March). Vietnamese Police Resolve To Prevent Child Sexual Abuse.
UNICEF. (2016). <u>Child protection in the digital age. National responses to online child sexual abuse and exploitation in ASEAN Member States.</u> Bangkok: UNICEF EAPRO.

^{130.} Viet Nam. (2021, 1 June). Decision 830/QD-TTg 2021 Program on support for children in the cyber environment 2021–2025.

^{131.} Socialist Republic of Viet Nam. (2021). Decree No. 716/QD-BTTTT dated May 26, 2021.

^{134.} Based on the Ministry of Education and Training's Decision No. 2972/QD-BGDDT dated September 24, 2021 to implement Decision No. 830/ QD-TTg dated June 1, 2021 of the Prime Minister approving the Program "Protecting and supporting children to interact healthily and creatively in the cyberspace in the period of 2021-2025".

^{135.} UNICEF. (2016). <u>Child protection in the digital age. National responses to online child sexual abuse and exploitation in ASEAN Member States.</u> Bangkok: UNICEF EAPRO.

^{136.} Vietnam Association for Protection of Child's Rights & ECPAT International. (2019). Sexual Exploitation of Children in Viet Nam Submission to the Human Rights Council.

^{137.} ASEAN (2019). Ending Violence Against Children in ASEAN Member States. Mid-term review of priority areas under the ASEAN Regional Plan of Action on the Elimination of Violence against Children 2016–2025.

^{138.} UNICEF Viet Nam, UNICEF Office of Research – Innocenti & University of Edinburgh (2016). Understanding The Drivers of Violence Affecting Children in Viet Nam.

^{139.} ECPAT International, Plan International, Save the Children, UNICEF and World Vision (2014). <u>National Child Protection Systems in the East Asia</u> and Pacific Region: A review and analysis of mappings and assessments.

In 2016, UNICEF noted the shrinking extended family support system, increasing economic migration and new threats such as trafficking and OCSEA. These trends make it imperative that the institutions responsible for child protection in Viet Nam be strengthened, training provided for social workers at all levels and referrals and services throughout the country enhanced.¹⁴⁰ In another, more recent study, UNICEF observed limited counselling services and shelters available for child (and women) victims of violence, with the available services mostly in urban areas.¹⁴¹

3.4.2 Civil society

International and national NGOs working on OCSEArelated issues in Viet Nam include the following:

- The **SecDev Foundation** is a Canadian-based think tank with the mission of ensuring that everyone has the right skills and knowledge to protect themselves from digital harm and take advantage of the emerging opportunities of the global digital economy. In Viet Nam it runs the *Digital Citizenship Viet Nam Initiative*¹⁴² which aims to promote digital safety techniques, foster digital literacy skills and conduct surveys about young people's online experiences.¹⁴³
- ChildFund Viet Nam is another international NGO working on online safety. The *Swipe Safe* project run by ChildFund Viet Nam from July 2017 to June 2020 with a grant from the Fund to End Violence against Children was implemented in 35 Vietnamese schools reaching 12,000 teenagers in the poorest regions of northern Viet Nam with knowledge about potential online risks including sexual abuse and how to use the internet wisely.¹⁴⁴

Monitoring data showed that 91% of the children demonstrated increased knowledge about privacy settings, information checks, responsible sharing, online searching and reporting harmful content, while 89% knew where to find support and 30% felt safer online.¹⁴⁵

- Under the project *Tackling online child sexual* exploitation in Viet Nam run by World Vision International in Viet Nam between March 2018 and February 2021, a project orientation workshop was conducted for 32 government leaders and officers from 15 departments and organisations in Da Nang in March 2019.¹⁴⁶
- The **Vietnet** Information and Communication Technology Center aims to narrow the digital gap and help communities take advantage of IT opportunities. In 2017, together with the Research Center of Management and Sustainable Development, the Vietnet Information and Communication Technology Center hosted a series of events as part of its *Digital Citizenship* programme that focused on the topic of online safety for children and the teaching of online safety in schools. A training course on *Online Safety for Children* was provided for social workers and caregivers, during which trends in OCSEA were discussed and guidance was provided on how to protect children against it.
- The Management Research Institute for Sustainable Development aims to develop the civil society sector and promote the rights of marginalised groups, especially children, youth, women and people with disabilities. In 2020, the institute conducted a survey among children and youth to assess their behaviour and risks online.¹⁴⁷

Two Years of Supporting Solutions: Results from the Fund's Investments.

^{140.} UNICEF Viet Nam, UNICEF Office of Research – Innocenti & University of Edinburgh (2016). Understanding The Drivers of Violence Affecting Children in Viet Nam.

^{141.} UNICEF, UN Women, UNFPA. (2020). A rapid assessment on violence against women and children (VAWC) as an impact of COVID-19 crisis and support needs for designing targeted communication activities and responses, 30.

^{142.} SecDev Foundation (n.d.) <u>Digital Citizenship Vietnam.</u>

^{143.} SecDev Foundation (n.d.) Using Manga to Teach Digital Safety in Vietnam: Black Rose Book Launch.

^{144.} Funded by the End Violence Fund through its Safe Online Initiative. ChildFund Viet Nam. (n.d.) <u>Helping children to navigate online world.</u> 145. Broadband Commission for Sustainable Development. (2019). Child Online Safety: Minimizing the Risk of Violence, Abuse and Exploitation Online.

^{146.} Funded by the End Violence Fund through its Safe Online Initiative. Global Partnership to End Violence Against Children. (2018).

^{147.} Research Center for Management and Sustainable Development. (2020). "Safe and smart digital technology for Asia – Promoting digital information security, citizenship and choice of Asian online consumers."

- Viet Nam Internet Association¹⁴⁸ brings together organisations, companies and individuals engaged in internet service supply and development. It aims to raise public awareness on internet use, reduce the digital divide and serve as a communication platform between the authorities, the Information and Communications Technology industry and society.¹⁴⁹ The prevention of OCSEA was discussed during the launch in 2017 of their #Netsmart handbook for adults on how to protect children from sexual abuse on the internet.¹⁵⁰ The #Netsmart handbook is written for caregivers and combines advice from psychologists and police with the stories of individuals who have been abused.
- The Viet Nam Association for Protection of Child's **Rights** is a network of individuals and organisations aiming to ensure the basic rights of children. In 2019, the Viet Nam Association for Protection of Child's Rights conducted three training activities for 120 staff members of child protection associations. The training covered the legal basis for protecting children online and basic skills for children and caregivers to protect children online. Moreover, in the years 2019–2021, the Viet Nam Association for Protection of Child's Rights conducted two research projects related to violence and child abuse: "Legal regulations on examination of children subjected to violence and abuse" supported by Save the Children and published in 2020 and "Survey on current situation of the implementation of friendly proceedings procedure and medical support for sexually abused children in Hanoi" supported by EU, JOLI JIFF Foundation for Judicial Initiatives and to be published in 2021.

3.4.3 Internet service providers and platforms

Collaboration with internet and mobile service providers and platforms is essential to investigate crimes and prevent the dissemination of CSAM. The legal requirements and practical procedures differ depending on whether the operators are Vietnamese or global.

Domestic Internet Service Providers

Evidence gathering: When the law enforcement authorities need evidence from a domestic service provider – for example, to identify who was using a particular IP address or phone number at the time an offence was committed – they serve a court order on the service provider demanding this information. They can then use the subscriber information to locate and apprehend the suspect and to submit as evidence in court.¹⁵¹

Removing/reporting CSAM: The Cyber Information Security Law imposes a legal duty on information system administrators and online service providers to delete information whose content may cause harm to children, mistreat them or otherwise infringe their rights, and to promptly notify (report to) and coordinate with the Cyber Task Force under the Ministry of Public Security for resolution.¹⁵² In accordance with this Law and the Law on Children, agencies, organisations and individuals participating in activities online are responsible for coordinating with the competent public bodies to guarantee children's rights online and preventing (blocking) content causing harm to children.¹⁵³ The Cyber Task Force and other agencies are responsible for taking measures to preclude, discover, prevent and strictly deal with the use of internet.¹⁵⁴

148. See Viet Nam Internet Association: https://via.org.vn/en/Thu-Ngo.

- 149. See Viet Nam Internet Association: https://via.org.vn/en/Thu-Ngo.
- 150. See Save the Children. 28 November 2017. 'Netsmart' booklet launch.

151. This approach however ignores challenges posed by carrier grade Network Address Translation, a process by which rapidly exhausting IPv4 addresses have been assigned by ISPs to multiple users at the same time, thereby precluding definitive identification of the device and user behind an IP address in certain cases.

- 152. Socialist Republic of Viet Nam. (2018). Cyber information Security Law No. 24/2018 / QH14, Article 29(2).
- 153. Socialist Republic of Viet Nam. (2018). Cyber Information Security Law No. 24/2018 / QH14, Article 29(3).

^{154.} Socialist Republic of Viet Nam. (2018). Cyber Information Security Law No. 24/2018 / QH14, Article 29(5).

In addition, the activities prohibited by Decree No. 72/2013/ND-CP on the management, provision and use of Internet services and online information include the propagating and inciting of pornography (not specifically CSAM).¹⁵⁵ Aggregated information websites are obliged to monitor and remove information and materials prohibited by this decree.¹⁵⁶ Similarly, social network companies are requested not to share pornography and to coordinate with State agencies to remove or block such material.¹⁵⁷ Owners of public internet access points¹⁵⁸ and public gaming points are mandated to post the list of prohibited acts on their internet services and not to allow their users to commit such acts.¹⁵⁹

Global platforms

Evidence gathering: If a report is made to the Vietnamese police about OCSEA on a global platform, such as Facebook, a request is made to the platform to obtain subscriber information and IP data. Once the IP is known, the police then follow the domestic internet service provider request process to resolve the IP data and confirm the identity, location and other details of the suspect. During the first consultation with the government on this report,¹⁶⁰ the representative from the Ministry of Information and Communications remarked that data sharing by the global platforms can be difficult.

Removing/reporting CSAM: With respect to removing/reporting CSAM, there are rarely any formal agreements between national law enforcement agencies and global platforms. The platforms would prefer to view requests from government partners as notifications of potential violations of their own terms of service. Since CSAM is contrary to the platforms' terms of service and the laws of their own countries (U.S. law), it would be in the companies' interests to remove such content. Interestingly, Decree No.72/2013/ND-CP explicitly indicates that its provisions also apply to foreign organisations and individuals "directly engaged in or related to the management, provision and use of Internet services, online information, and online games, and assurance of information safety and security." ¹⁶¹

In 2017, 2018 and 2019, the transparency reports of major social media platforms show that authorities in Viet Nam made:

- 2,041 requests to Facebook for content restriction, including 1,556 in the second half of 2018 alone. The reasons for requesting content restriction in Viet Nam included opposition to the Communist Party and government, promotion of unauthorised public demonstrations, defamation of public officials, spread of false information, and trade in wildlife and regulated products.
- 38 requests for Facebook user data;
- 9,066 requests to Google for content removal, of which 6,316 concerned criticism of the government and 2,172 concerned national security. Of the remainder, eight concerned obscenity/ nudity on YouTube.
- 3 requests for Google user data
- 2 requests to Apple for user data, and 5 requests to remove a total of 75 apps from the App Store;
- No requests to Twitter for user data or content removal.

^{155.} Socialist Republic of Viet Nam. (2013). Decree No. 72/2013/ND-CP on the management, provision and use of Internet services and online information, Article 5.

^{156.} Socialist Republic of Viet Nam. (2013). Decree No. 72/2013/ND-CP on the management, provision and use of Internet services and online information, Article 24(4).

^{157.} Socialist Republic of Viet Nam. (2013). Decree No. 72/2013/ND-CP on the management, provision and use of Internet services and online information, Article 25 (5) and (6).

^{158.} Public Internet access points are defined as: "a) Locations that an Internet agent has the lawful right to use for service provision; b) Public Internet access points of an enterprise under the direct management of member units or individuals who represent an internet service provider where the Internet access service is provided to Internet users; c) Public Internet access points in hotels, restaurants, airports, harbors, bus stations, coffee shops and other public places, which organisations and individuals have the lawful right to use for providing Internet access services to Internet users." Socialist Republic of Viet Nam. (2013). Decree No. 72/2013/ND-CP on the management, provision and use of Internet services and online information. Article 3(6).

^{159.} Socialist Republic of Viet Nam. (2013). Decree No. 72/2013/ND-CP on the management, provision and use of Internet services and online information, Articles 9 and 36.

^{160.} National Consultation on *Disrupting Harm* with government representatives on 19 October 2021.

^{161.} Socialist Republic of Viet Nam. (2013). Decree No. 72/2013/ND-CP on the management, provision and use of Internet services and online information, Article 2.

4. HOW TO DISRUPT HARM IN VIET NAM

Disrupting harm from online child sexual exploitation and abuse requires comprehensive and sustained actions from us all – families, communities, government representatives, law enforcement agencies, justice and social support service professionals and the technology and communications industry. While children are part of the solution, the harm caused by OCSEA obliges adults to act to protect them; we must be careful not to put the onus on children.

A set of actions needed in Viet Nam are clustered under four key insights and signposted for different stakeholder groups. All these recommended actions are interlinked and are most effective if implemented together. The recommendations are based on the limited data accessible to the *Disrupting Harm* team rather than on a comprehensive picture of OCSEA in the country.

4.1 FOUR KEY INSIGHTS AND RECOMMENDATIONS FOR ACTIONS

Disrupting Harm alignment with the Model National Response

Many countries, companies and organisations have joined the WePROTECT Global Alliance to prevent and respond to online child sexual exploitation and abuse. As a member of the Global Alliance, Viet Nam can use the Model National Response to Preventing and Tackling Child Sexual Exploitation and Abuse to help organise its response to OCSEA. The Model is a valuable tool for governments to organise and improve the level of their response. Most of the recommendations in this report align with the 21 'capabilities' articulated in the Model National Response, but Disrupting Harm identifies priority areas for interventions based specifically on the data about the Vietnamese situation. Most Disrupting Harm recommendations refer to legislation,¹⁶² dedicated law enforcement,¹⁶³ judiciary and prosecutors,¹⁶⁴ and education programmes.¹⁶⁵ All recommendations are practical, evidence-based and actionable. Disrupting Harm has indicated for whom the recommendations are formulated, i.e., for government representatives, law enforcement, justice actors, the internet and technology industry, caregivers, community, and teachers to protect children from these crimes.

More recently, the Association of Southeast Asian Nations (ASEAN) endorsed the *Regional Plan of Action for the Protection of Children from All Forms of Online Exploitation and Abuse in ASEAN*¹⁶⁶ which includes commitments for member states to strengthen online child protection in the region. The plan includes seven focus areas including awareness raising, strengthening data collection, and legislative reform, among others. The Disrupting Harm recommendations detail sustained, practical, and evidence-based activities that can be implemented in Viet Nam as part of their commitment to the Regional Plan of Action.

INSIGHT 1

A large majority of children in Viet Nam have access to the internet, and most of these children go online every day. This is also the case for caregivers. However, only about one third of children have received some form of online safety training.

Government

1.1 Mandate the Ministry of Information and **Communications – through the Multi-agency** and Interdisciplinary Network to Protect and Rescue Children in the Online Environment to lead the implementation of the newly-adopted National Programme on Child Online Protection. Both the Network and the National Programme are two highly promising initiatives for combating OCSEA. Review programmes and plans periodically in line with emerging evidence and feedback from all relevant authorities, frontline workers and communities. Ensure that appropriate institutional arrangements are in place to develop and maintain coordination mechanisms, planning, budgeting, monitoring and reporting. Liaise with international organisations and civil society and draw on their knowledge and experience.

1.2 Integrate efforts to tackle OCSEA into additional structures and programmes that address other forms of child exploitation and abuse, rather than exclusively designing, planning and implementing programmes for OCSEA. Bearing in mind that children are often exposed to the same kinds of actual or potential sexual exploitation and abuse in both online and offline settings, and that the same persons may be responsible in both cases. An effective child protection system is a prerequisite for combating OCSEA.

^{162.} Model National Response #3.

^{163.} Model National Response #4.164. Model National Response #5.

^{165.} Model National Response #3.

^{166.} Association of Southeast Asian Nations. (2020). <u>Regional Plan of Action for the Protection of Children from All Forms of Online Exploitation</u> and Abuse in ASEAN: Supplement to the ASEAN Regional Plan of Action on the Elimination of Violence Against Children.

1.3 Ensure national-scale public awareness and education about sexual exploitation and abuse of children – including how technology might play a role. Existing and new awareness and education programmes need to be taken to scale to ensure their messages reach all people. Materials should be developed and tested through safe and ethical consultations with children, caregivers and teachers, to ensure they address their lived experiences of online risks. These materials should also include the tips and techniques that children can use to keep themselves safe. Key objectives should include:

- Reaching children of all ages who access the internet, especially now that in COVID times children are shifting to online learning at an earlier age even from grade 1.
- Promote safe digital environments to be created by industry and to be used by caregivers.
- Equipping caregivers with the knowledge and skills to foster safe and ongoing communication with children about their lives online (see *Start the Chat*¹⁶⁷ for an example).
- Fostering social and family norms that facilitate positive and healthy perception and conversations about sex. Foster behaviours that encourage girls, boys, and adults to disclose, report and seek help about child sexual exploitation and abuse, and which minimise embarrassment and shame or negative perceptions about the consequences of reporting.
- Strengthening children's digital literacy (such as the *Swipe Safe*¹⁶⁸ project) to provide them with the skills and understanding needed to avoid or navigate dangerous situations online. This could include lessons about how to block an individual and report inappropriate content or requests.

- Ensuring children are aware of the risks inherent in online interaction and the exchange of personal information, images and videos.
- Ensuring specific actions to prevent and respond to children with a disability being subjected to OCSEA.

When children do not know about sex, it enables offenders to take advantage. We must ensure that knowledge reaches all children, and includes information about sex, consent, personal boundaries; what adults or others around children can or cannot do to them; risks and responsibilities when taking, sending, and receiving sexual images; and how to say no to and report inappropriate behaviour. This will help children to identify risky or inappropriate interactions both online and in person, empower them to protect themselves and teach them what to disclose. Reports¹⁶⁹ and initiatives¹⁷⁰ that can serve as good starting points, and there are good examples of age-appropriate resource material.¹⁷¹

Caregivers, teachers, medical staff, and social support services¹⁷²

1.4 Help children, caregivers, teachers and those working with children understand the

full extent of the risks of sharing sexual content and how to engage in harm minimisation to limit possible negative repercussions. Most children who shared sexual content initially did so because they were in love or trusted the other person, but this behaviour can lead to serious harm, such as non-consensual sharing of the content with others and sexual extortion.

169. UNFPA. (2021). <u>My Body is My Own</u>.

^{167.} See: The Australian eSafety Commissioner's programme '<u>Start the Chat</u>' <u>to encourage caregivers to talk with their children about their lives online.</u> 168. Funded by the End Violence Fund through its Safe Online Initiative. ChildFund Viet Nam. (n.d.) Helping children to navigate online world.

^{170.} UNGEI. (2020). Bodily autonomy and SRHR.

^{171.} NSPCC. (2017). Talk PANTS with Pantosaurus and his PANTS song #TalkPANTS - YouTube.

^{172.} Government, inter-governmental agencies, and civil society need to translate and convey these messages to reach caregivers, teachers, medical staff and social support workers.

INSIGHT 2

Internet-using children in Viet Nam are already being subjected to OCSEA. The data from the household survey suggest that there is considerable awareness of OCSEA risks among children and caregivers, but disclosure, seeking help and reporting to formal mechanisms is very low.

Government

2.1 Increase the availability and effectiveness of reporting mechanisms and ensure that helpline III can provide the required functions of a hotline and helpline or, alternatively, appoint an agency that can function as a hotline, i.e., to remove child sexual abuse material from the internet. Continue the system adopted in 2020 by helpline III to disaggregate OCSEA cases to enhance future evidence-based policy, but ensure the definition of OCSEA is in line with this report.

2.2 Diversify mechanisms for children to disclose concerns, seek help and formally make reports (including simple child-friendly, online methods, e.g., through a chat channel as already planned by helpline 111), bearing in mind that most children first prefer to seek help from friends, then within their own family or community. Make sure children are aware of these mechanisms. Children's failure to speak out is a major reason why OCSEA often remains hidden from view and not investigated and stopped.

2.3 Invest in improving the capacity of the social service workforce. This may include the recruitment and training of sufficient professional child protection officers working at local levels, the clarification of responsibilities and procedures, and an increase in

the supply of services, particularly in rural areas and

less developed regions.

2.4 Improve the capacity of frontline staff in contact with children to better identify children at risk or that have experienced OCSEA. This should include teachers, staff in schools as well as health workers, in addition to all those providing psychosocial support.

Caregivers, teachers, medical staff and social support services¹⁷³

2.5 Foster safe and ongoing communication between children and trusted adults about their lives online (and offline). Normalising communication about online activities will increase the likelihood that children will disclose any concerns, risks and harmful experiences they may face.

2.6 Responses to disclosures of OCSEA should always convey that it is never the child's fault,

whatever choices they have made. It is always the fault of the adult abusing or exploiting the child. *Disrupting Harm* shows that children subjected to OCSEA often blame themselves and feel that they have let their caregivers and others down. Responses should be without judgement or punishment. For example, see the WHO guidelines on first line response to child maltreatment.¹⁷⁴

2.7 Inform children about the existence of hotlines

and helplines and other help-seeking channels and let them know that these are safe ways for them to disclose difficult experiences and find advice and support which they may not be comfortable about disclosing to people in their family or community (particularly as the offenders may be family or community members). An important prerequisite of this recommendation is that hotlines and helplines are adequately staffed, resourced and able to respond effectively.

^{173.} Government, inter-governmental agencies, and civil society need to translate and convey these messages to reach caregivers, teachers, medical staff and social support workers.

^{174.} World Health Organization. (2021). WHO Guidelines for the health sector response to child maltreatment.

Industry

2.8 Social media and chat platforms, such as Facebook, should work proactively to prevent sexual content from appearing on children's feeds and where relevant adhere to government regulations on how to do so. Internet service providers should be legally and explicitly obliged to filter and remove CSAM. Enforcing this obligation is vital in keeping children safe online.

2.9 Prioritise children's needs in product development processes. Such design must be informed by evidence on children's digital practices and their experiences of online child sexual exploitation and abuse, including this *Disrupting Harm* study.¹⁷⁵

2.10 Make formal reporting mechanisms within social media and chat platforms clear and accessible to children and detail in child-friendly terms what the process looks like after children submit a report. Platforms and service providers must respond rapidly to reports made by children and demonstrate transparency and accountability.

Considerations for future research

- The survey did not include younger children aged 6–11 years. Future studies could consider including this younger group to capture their perspective and experiences. However, necessary measures and caution should be taken as the questions might be too sensitive for them to answer.
- 2. Teachers were not included in the survey. Future studies could consider including a teacher module to capture their perspectives and experience on the topic as 98 percent of the children surveyed were school going. Teachers regularly and directly interact with students in a school setting.

INSIGHT 3

Law enforcement systems are in place. establishing a specialised unit and strengthening capacity through training could improve the overall response.

Law enforcement

3.1 Prioritise and allocate resources to a specialised unit and invest in the training of police officers on how to address OCSEA within their respective investigations and build evidence for prosecutions. Address child protection issues – including OCSEA – through training, and provide specialist training more widely. Provide both initial and refresher trainings.

3.2 For the Ministry of Public Security to allocate talent and resources to prevent, manage and respond to OCSEA. Ensure that the law enforcement authorities have sufficient personnel appropriately supported with tools and equipment, knowledge and skillset training to look proactively for early warning signals and adopt enhanced techniques in intelligence gathering and evidence building for the successful prosecution of OCSEA cases.

3.3 Actively engage in international cooperation to provide oversight to prevent child sex offenders travelling, including through border management and control, in conjunction with other relevant ministries in the country and beyond.

3.4 Prioritise the re-connection of the INTERPOL International Child Sexual Exploitation (ICSE) Database to Viet Nam, followed by a refresher training on victim identification and use of the database.

3.5 Regularly gather, share and analyse information and intelligence from disaggregated data on child sexual exploitation and abuse reports (both online and offline) in order to understand the scope of threats and the pattern of offending. Prioritise international referrals such as those from INTERPOL, which regularly reaches out to national law enforcement authorities with referrals on intelligence pertaining to eminent threats on OCSEA.

^{175.} A good starting point for exploration are the free tools made available by the Australian eSafety Commissioner as well as well as this <u>framework</u> developed by UNICEF.

INSIGHT 4

access to services.

Some child-friendly court processes are provided for in laws and policies but important OCSEA-related legislation, policies and standards are not yet enacted in Viet Nam. Further research is needed to assess the experiences of accessing justice by victims of OCSEA.

4.1 Conduct research on the response of the justice sector to OCSEA and access to justice for victims of OCSEA. The *Disrupting Harm* partners were not granted government permission to conduct part of their research in Viet Nam, but it remains important to understand if OCSEA victims have access to justice, including child friendly justice, compensation and

4.2 Mandate the Multi-agency and Interdisciplinary Network to Protect and Rescue Children in the Online Environment to provide further advice on changes to the legal framework and develop proposed amendments in support of the response to the following recommendations.

 Amend legislation to provide a clear and specific definition of child sexual abuse material (CSAM) and to criminalise conduct related to it specifically, with penalties commensurate with the crime.
While the Criminal Code criminalises conduct related to pornographic content in general, its provisions fail to define CSAM. In addition, no special protection is afforded to children and the penalties are not commensurate with CSAMrelated crimes.

- Amend legislation to specifically criminalise grooming, the live-streaming of child sexual abuse for children all ages, sexual extortion committed in the online environment and online sexual harassment specifically.
- Amend legislation to bring it fully into line with international standards set by the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography, the Convention on the Protection of Children Against Sexual Exploitation and Sexual Abuse of the Council of Europe (Lanzarote Convention) and Convention on Cybercrime (Budapest Convention). The Lanzarote Convention and Budapest Convention better address current manifestations of OCSEA and thus provide useful guidance for national legal frameworks. Furthermore, they are open to accession by states which are not members of the Council of Europe.

This comprehensive report is the result of a two-year collaborative effort to design research, gather data and produce extraordinary evidence. These efforts would not have been possible without the engagement of individuals and partners in Viet Nam. First and foremost, our biggest thanks go to the children who contributed – especially the young people who had experienced OCSEA and courageously spoke of it with the research teams. The experiences of children are key to understanding and guiding our way forward. The project partners would also like to express their appreciation to everyone who engaged with *Disrupting Harm* by:

Contextualising the findings:

Ministry of Information and Communication (MIC); Department of Children's Affairs including Child Helpline, MOLISA; Call Center – Hotline III, Department of Culture and Education of the National Assembly; Department of Science, Education, Culture and Social Affairs of the Government's Office; UNICEF Viet Nam Office, UNICEF East Asia and Pacific Regional Office, Viet Nam Association for Protection of Child Rights (VACR); Department of Cyber Security and INTERPOL, INTERPOL NCB, Ministry of Public Security; Ministry of Education and Training; Ministry of Culture, Sports and Tourism, Pioneer's Council; ChildFund, World Vision International and UNICEF Viet Nam.

• Supporting data collection:

Cyber-crime prevention department, National Central Bureau Hanoi, National Police Investigation Agency, Office of the Criminal Investigation Department, Office of the Child Sexual Abuse Division, Office of the Cyber–Crime Investigation Division, Ipsos Viet Nam, Ipsos MORI.

ECPAT, INTERPOL, and UNICEF Office of Research – Innocenti have appreciated the unique opportunity to work shoulder-to-shoulder to assess online child sexual exploitation and abuse. Without the collaborative effort of all involved in the development of the reports, this tremendous piece of research would not have come together. In particular, we would like to thank:

ECPAT International:

Tiago Afonso, Dr Victoria Baines, Alice Beaven, Will Beaven, Willy Buloso, Yermi Brenner, Dr Mark P. Capaldi, Narciso Cumbe, Dr Dorothea Czarnecki, Jarrett Davis, Rangsima Deesawade, Julia Durska, Sonia Espallargas Val, Anneka Farrington, Beatrice Gacengo, Thiyagu Ganesan, Dr Susanna Greijer, Zipporah Goetze, Supriya Kasaju, Josefin Hagstrom, Alastair Hilton, Bernard Kennedy, Maria Ibañez Beltran, Worrawan Jirathanapiwat, Dr Mark Kavenagh, Dorine van der Keur, Susan Kreston, Guillaume Landry, Marie Laure Lemineur, Raphaelle Lecler, Katrina Mariswamy, John McGill, Mark McKillop, Stella Motsi, Florence Mueni, Thomas Müller, Manida Naebklang, Cathrine Napier, Rumbidzai Naindi, Freddie Nickolds, Megan Northey, Esther Obdam, Dr Nativity Petallar, Dr Kirsten Pontalti, Marie Joy Pring, Dr Ethel Quayle, Marita Rademeyer, Kieran Rumsby, Jennifer Schatz, Guncha Sharma, Nong Socheat, Andrea Varrella, Chitrapon Vanaspong, Kirsten Walkom, Timothy Williams.

UNICEF Office of Research – Innocenti:

David Anthony, Dr Daniel Kardefelt-Winther, Marie Nodzenski, Marium Saeed, Rogers Twesigye.

INTERPOL's Crimes against Children Unit

The partners also acknowledge the guidance of the <u>Panel of Advisors</u> and the extraordinary financial investment in this project from the <u>Global Partnership to End Violence against</u> <u>Children</u>, through its Safe Online initiative. The <u>Disrupting Harm</u> partners are grateful to the Safe Online team for its conceptualisation of <u>Disrupting Harm</u>, its technical contributions, and its unwavering support.

