

ONLINE VIOLENCE AGAINST CHILDREN IN SRI LANKA:

A National Research on Incidence, Nature and Scope

Summary Report



State Ministry of Women and Child
Development, Pre-School & Primary
Education, School Infrastructure &
Education Services



End Violence
Against Children



Save the Children

World Vision



leads
Where Children Come First...





State Ministry of Women and Child
Development, Pre-School & Primary
Education, School Infrastructure &
Education Services

Mandate of the State Ministry of Women and Child Development, Pre-Schools & Primary Education, School Infrastructure & Education Services

A strong nation of women and children with ensured rights that contributes towards sustainable development



Save the Children

Mandate of SCI

'Save the Children works in more than 120 countries to contribute to immediate and lasting improvements for children, in emergencies as well as development contexts. We want a world in which all children survive, learn and are protected. Through our work we strive towards achieving three breakthroughs in the way the world treats children; No child dies from preventable causes before their fifth birthday; All children learn from a quality basic education; and Violence against children is no longer tolerated'.



Mandate of World Vision

'World Vision is a Christian, relief, development and advocacy organization dedicated to working with children, families and communities to overcome poverty and injustice.

We work through our main sectors – education, health and nutrition, water and sanitation, economic development and child protection – serving all people, regardless of religion, race, ethnicity or gender. World Vision is committed to protecting children from harm so that every child has the essential foundations for life in all its fullness.'

Disclaimer

The views and opinions expressed herein are those of the contributors, and do not necessarily reflect the views of the State Ministry of Women and Child Development, Save the Children and World Vision Lanka.

All Rights Reserved

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise without the prior written permission of the publisher.

Suggested Citation:

Fernando, N., Hakeem, M.A.M., Seneviratne, W., De Silva, M., Cooray, J (2021), Online Violence Against Children in Sri Lanka: A National Research on Incidence, Nature and Scope. State Ministry of Women and Child Development, Pre-Schools & Primary Education, School Infrastructure & Education Services – Sri Lanka, Colombo.

Published by: State Ministry of Women and Child Development, Pre-Schools & Primary Education, School Infrastructure & Education Services, Sri Lanka.

ISBN: 978-624-5738-01-4

© State Ministry of Women and Child Development, Pre-Schools & Primary Education,
School Infrastructure & Education Services

© Save the Children © World Vision

Acknowledgments

The study on “The Incidence, Nature and Scope of Online Violence Against Children in Sri Lanka”, was conducted by Social Policy Analysis and Research Centre (SPARC) of University of Colombo and was commissioned by the **State Ministry of Women and Child Development, Pre-Schools & Primary Education, School Infrastructure & Education Services** in collaboration with Save the Children and World Vision Lanka. The input and support provided by government and non-government stakeholders, children and all other interviewees for this research is acknowledged with sincere appreciation. The actual names of the participants are replaced with pseudonyms to protect their identities.

This research was made possible through support provided by the Global Partnership to End Violence Against Children (GPEVAC).

Steering, Leadership and Guidance

Mrs. K.M.S.D. Jayasekara

Secretary – State Ministry of Women and Child Development, Pre-Schools & Primary Education, School Infrastructure & Education Services

Mrs. Darshana Senanayake

Former Secretary – Ministry of Women and Child Affairs, and Dry Zone Development

Ms. N.H.M.W.W. Herath

Additional Secretary (Development) – State Ministry of Women and Child Development, Pre-Schools & Primary Education, School Infrastructure & Education Services

Ms. Sujeewa Palliyaguruge

Director Development – State Ministry of Women and Child Development, Pre-Schools & Primary Education, School Infrastructure & Education Services

Mrs. P. Chandima Sigera

Former Commissioner – Department of Probation and Child Care Services

Ranjan Weththasinghe

Director – Policy, Advocacy & Research, Save the Children, Sri Lanka

Buddhini Withana

Senior Technical Advisor – Child Protection, Save the Children, Sri Lanka

Authors

Dr. Nishara Fernando

M.A.M. Hakeem

Prof. Wasantha Seneviratne

Malith De Silva

Jerome Cooray

Core Research Team

Dr. Nishara Fernando

Principal Sociologist/Director SPARC – University of Colombo

M.A.M. Hakeem

Principal Legal Analyst

Prof. Wasantha Seneviratne

Child Safeguarding Focal Point & Legal Advisor

Malith De Silva

Sociologist/Research Coordinator

Jerome Cooray

Political Geographer/Consultant Research Manager

Shiromi Samarakoon

Project Manager – End Online Violence Against Children, Save the Children

M. H.A.D.D. Lakshantha

National Campaign Coordinator – End Violence Against Children, World Vision Lanka

Sampath Chandrasena

Cyber Security Analyst

Dr. Mahinda Pushpakumara

Quantitative Analyst

Umair Naseef

Tri-lingual Assistant Research Coordinator

Devaneshan Raju

Tri-lingual Assistant Research Coordinator

Chandani Peiris

Development Officer & the District Child Rights Promotion Officers of the Department of Probation and Child Care Services

Technical Advisors

Buddhini Withana

Senior Technical Advisor – Child Protection, Save the Children, Sri Lanka

Ranjan Weththasinghe

Director – Policy, Advocacy & Research, Save the Children, Sri Lanka

Kanishka Rathnayake

Regional Campaign Advisor – Advocacy & External Engagement – Asia & Pacific, World Vision International (former Technical Advisor – Child Protection & Participation, World Vision Lanka)

M. H.A.D.D. Lakshantha

National Campaign Coordinator – End Violence Against Children, World Vision Lanka

Nayomi Silva

Manager – Advocacy, LEADS & National Coordinator – National Partnership to End Violence Against Children, Sri Lanka (NPEVAC)

Acknowledgments

Petricia R. Wijetunge

Legal Officer cum Advocacy Coordinator – LEADS

Wijesena Withana

Consultant Legal and Law Enforcement Advisor – Consortium to End Online Violence Against Children, Sri Lanka

Ayesh S.I. Kirige

Consultant Cybercrime Investigator – Consortium to End Online Violence Against Children, Sri Lanka

Ishadi M. Gulawita

Consultant Cybercrime Analyst – Consortium to End Online Violence Against Children, Sri Lanka

International Expertise

Kuno Sørensen

Psychologist and Former Senior Advisor – Save the Children, Denmark

John Zoltner

Senior Advisor – Technology for Development & Innovation, Save the Children International

Daniel Kardefelt-Winther

David Finkelhor

Ethical Review, and Guidelines and Training on Child Safeguarding During Research

Ethical Review and Approval

Ethics Review Committee, Faculty of Arts, University of Colombo

Buddini Withana

Author – National Guidelines on Conducting Research with Children in Sri Lanka & Key Advisor on Child Safeguarding of this study

Prof. Wasantha Seneviratne

Primary Author – Child Safeguarding Risk Assessment Framework of this study & Child Safeguarding Focal Point during the period of the study

Child Safeguarding & Ethics Trainers:

Buddhini Withana, Chandrika Ramachandran, Ranjan Weththasinghe, Kanishka Rathnayake, M.H.A.D.D. Lakshantha

Editors

Jerome Cooray

Authors' Editor

Buddhini Withana

Key Editing Advisor & Developmental Editor

Ranjan Weththasinghe

Editing Advisor

Belinda Wise

Language & Copy Editor

Project Team – Save the Children, Sri Lanka

Ahila Thillainathan

Director – Programmes

Shyamali Gnanasena

Senior Programme Manager – Child Protection

Shiromi Samarakoon

Project Manager – End Online Violence Against Children, Sri Lanka

Buddhini Withana

Senior Technical Advisor – Child Protection

Ranjan Weththasinghe

Director – Policy, Advocacy & Research

Nirasha Perera

Senior Manager – Communications, Advocacy & Campaigns

Project Team – World Vision Lanka

Kanishka Rathnayake

Regional Campaign Advisor – Advocacy & External Engagement, Asia & Pacific, World Vision International (former Technical Advisor, Child Protection & Participation, World Vision Lanka)

Chandila Colombegge

Technical Advisor – Child Protection & Participation

M.H.A.D.D. Lakshantha

National Campaign Coordinator – End Violence Against Children

Jerome Cooray

Consultant Project Manager – Research, Consortium to End Online Violence Against Children, Sri Lanka

Abbreviations

KII	- Key Informant Interview
CSAM	- Child Sexual Abuse Material
NCPA	- National Child Protection Authority
ICT	- Information and Communications Technology
ISO	- International Standard Organization
CEOP	- Child Exploitation and Online Protection
NCA	- National Crime Agency
ISP	- Internet Service Provider
URL	- Uniform Resource Locator
DNS	- Domain Name System
BBFC	- British Board of Classification
UK	- United Kingdom
IWF	- Internet Watch Foundation
FBI	- Federal Bureau of Investigation
IINI	- Innocent Images National Initiative
IRC	- Internet Relay Chat
BBSs	- Bulletin Board Systems
ITU	- International Telecommunication Union
P2P	- Peer-to-Peer
COP	- Child Online Protection
NCMEC	- National Center for Missing & Exploited Children
ESP	- Electronic Service Providers
EU	- European Union
ASP	- Access Service Provider
VPN	- Virtual Private Network
DPI	- Deep Packet Inspection
OVAC	- Online Violence against Children
CRC	- Convention on the Rights of the Child
SDG	- Sustainable Development Goals
SDCS	- Sustainable Development Council of Sri Lanka
SLCERT	- Sri Lanka Computer Emergency Readiness Team
UN	- United Nations
ICTA	- Information and Communication Technology Agency
CID	- Criminal Investigation Department

Contents

Foreword	1
Message from the State Ministry of Women and Child Development, Pre-Schools, Primary Education, School Infrastructure and Educational Services	2
Message from SPARC	3
Message from Save the Children International, Sri Lanka	4
Message from World Vision Lanka	5
Executive Summary	6
Introduction	6
Methodology	6
The Incidence, Nature and Scope of Online/Cyber Violence against Children (OVAC) in Sri Lanka	7
Awareness of Online/Cyber Violence	8
The Role of Mass Media	9
Views of the Children Regarding the Existing Legal Mechanisms	9
Existing Technology-driven Response Mechanisms	10
Recommendations	11
Policy Reforms and Civic Awareness	11
Legal Reforms	11
Technology-driven Solutions	11
Cross-Sector Partnerships	11
Chapter 01 - Introduction	12
Chapter 02 - Context Review	14
2.1 Cyber-space: A New Spatial Realm	15
2.2 Cyber-space and Children: The Dangers	15
2.3 Children of Sri Lanka and Online Violence	16
Chapter 03 - Research Methodology	17
Data Collection	18
Review of secondary data	18
Data Collection Techniques – Children using internet	18
Sample Selection	19
COVID-19 Pandemic and the Contingency Plan	21
Sample selection for Expert Key Informant Interviews (EKI)	21
Analysis	21
Ethical Considerations: Doing Research with Children	21
Limitations of the Study	22
Chapter 04 - Findings: Incidence, Nature and Scope of Online Violence against Children in Sri Lanka	23
Demographic data	24
Expert definitions of online violence against children in Sri Lanka	27
Experiencing Online Violence	27
Child Sexual Abuse Material	28
Revenge Porn	28
Self-generated sexual content	29

Extortion of Children	29
Online Platforms and Experiencing Online Violence	30
Reaction of Children to Experiences of Online Violence	31
Help Seeking Behaviour	31
Reasons for Not Seeking Help	33
Fear	34
Unaccommodating Parent-Child Relationships	35
Lengthy Legal Process and Re-victimization in the Process	35
Difficulties in Accessing Legal Support	35
Characteristics that make children vulnerable to online violence	36
Gender of Children	36
Over confidence about internet use	36
Lack of parental supervision	36
Using internet for a long period	36
Sharing pictures and personal data on internet	37
The Impact of Online Violence on Children	37
Role of Mass Media	42
Chapter 05 - Online Violence, Law and Children of Sri Lanka	44
Brief Analysis of the Existing Legal Framework	45
Shortcomings of the Constitution of Sri Lanka	47
Shortcomings of the Children's Charter	47
Shortcomings of the Penal Code	47
Shortcomings of the Computer Crimes Act	48
Shortcomings of Policy	48
Law and the Voice of Sri Lankan Children	48
Chapter 06 - Global Technologies and Avenues Available for Sri Lanka: Tech-driven Approaches to Tackle Cyber/Online Violence Against Children	50
Global Tech-driven Avenues	51
Tech-driven Approaches Feasible for Sri Lanka	52
Chapter 07 - Recommendations	54
1. Policy and Governance	55
2. Criminal Justice	57
3. Victim support	57
4. Societal	58
5. Industry	59
6. Media and Communication	60
The Future	61
Bibliography	62
Annex 01	67
Annex 02	82
Annex 03	88



Foreword

When Save the Children was founded more than 100 years ago, children faced grave danger from all directions: millions became orphans in World War I and then millions more joined them when, just as the war ended, the global “Spanish Flu” pandemic struck. In 1920, children were prey to infectious diseases like Polio. They were not guaranteed an education. Many were forced to work long hours for nominal pay. They were subject to cruel punishment and abuse. In many cultures, they were often forced to marry in their early teenage years.

It pains me to say a century afterwards that, although we have made progress – most notably against Polio – all those threats still pose a danger to children around the world. Unfortunately, over the past 30+ years, we have added an entirely new threat: online violence against children. As Sri Lanka’s children and youth increasingly go online, they are able to enrich their lives by finding information about any topic, educating themselves and accessing economic opportunities. They can also entertain themselves with videos or games and interact socially. Taken together, those possibilities make the use of technology a tremendous draw for children. According to the “Survey on Social Media Security” report by the Sri Lankan Computer Emergency Readiness Team (SLCERT), 50% of Sri

Lankan youth were already spending 1 to 5 hours on social media platforms by 2017. Of course, that number is growing rapidly and, as it does, so does the level of risk faced by children.

When we seek to understand rapidly changing phenomena like the risks that children face online, Save the Children has a tried-and-true methodology: ask the children. I am happy to say that is exactly what my colleagues in Sri Lanka did when investigating the “Incidence, Nature and Scope of Online/Cyber Violence against Children.” The results were sobering.

Of the 1,911 children we interviewed for this study, more than 28% told us they had been the targets of online violence. Those children will tell you that online violence takes many forms, including cyber bullying (reported by 20.7% of children who experienced online violence), cyber extortion (also 20.7%), receiving sexually explicit images (28%) and many other harmful acts.

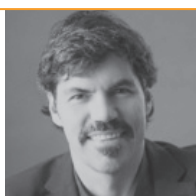
The children make it clear that those who we would expect are best-positioned to stop the online threats are not able to do so:

- 73% say their parents are not knowledgeable enough to supervise their internet use

- Though teachers might be able to fill that knowledge gap, 67% of children say they would not confide in an educator because they often blame the child for the online violence
- And most troubling of all: 92% say they would not take legal action against a perpetrator of online abuse.

The temptation is to say that the solution is to train the children to keep themselves safe: they should stop sharing private information, refrain from communicating with people they do not know in real life, keep their passwords and computers secure... We absolutely need to teach children to be safe online, but our answer to violence against children cannot be for children to study how to be less of a target for adults. We need systematic change.

After listening to the voices of children and a careful analysis of the issues, this report makes a series of concrete recommendations on what steps need to be taken in Sri Lanka – and around the world – to achieve that systemic change so we can keep our children safe in the digital spaces they will increasingly inhabit.



John Zoltner

Senior Advisor
Technology for Development and Innovation
Save the Children International



Save the Children

Message of the State Ministry of Women and Child Development, Pre-Schools & Primary Education, School Infrastructure & Education Services

The State Ministry of Women and Child Development, Pre-Schools & Primary Education, School Infrastructure & Education Services is delighted to present this publication of Sri Lanka's first ever national scale research on the 'incidence, nature and scope of online violence against children'. Online violence against children has become a rapidly growing issue in the recent past both globally and nationally due to the cyber-technological advancement we have experienced over the first two decades of the 21st century.

In 2018, in keeping with the Sri Lankan Government's national and global commitment to tackle all forms of violence against children, Sri Lanka became a path-finder country as a partner of Global Partnership to End Online Violence Against Children. As a path-finder country Sri Lanka has undertaken the commitment to develop new strategies to end all forms of violence against children in line with the United Nations Sustainable Development Goals 2030 Agenda.

Although there has been a common understanding regarding the issue of online violence against children, the lack of scientifically accrued data remained an obstacle in understanding the clear scope of this issue in Sri Lanka. Therefore in 2018, in line with Sri Lanka's aforementioned commitment as a path-finder country,

the Ministry commissioned the first ever national scale Project to End Online Violence Against Children in Sri Lanka. Alongside the Ministry and its integral units – the Department of Probation and Child Care Services (DPCCS) and the National Child Protection Authority (NCPA), the Save the Children International in Sri Lanka, World Vision Lanka and LEADS joined this nationally important initiative. As a key component of this project, the ministry commissioned this research on incidence, nature and scope of online violence against children in Sri Lanka in September 2019 under the technical leadership of Save the Children and World Vision Lanka. This research was conducted by the Social Policy Analysis and Research Centre (SPARC) of the University of Colombo.

The key finding of this research, that three out of ten participant children (30% out of over 1900 children) have experienced at least one form of online violence is crucially alarming. This indeed calls for effective and rapid response on the part of our ministry and other key stakeholders. The findings and recommendations of this research have bolstered the commitment of the Government and Ministry to end online violence and all other forms of violence against our children in Sri Lanka, in collaboration with all the key stakeholders including the law enforcement, civil society, industry and academia.



As a path-finder country Sri Lanka has undertaken the commitment to develop new strategies to end all forms of violence against children in line with the United Nations Sustainable Development Goals 2030 Agenda

The Ministry renders its sincere thanks to the Global Partnership to End Online Violence Against Children (GPEVAC) for its generous funding support, Save the Children and World Vision Lanka for their technical support, and the SPARC – University of Colombo for successfully conducting this research. Furthermore, the Ministry wishes to thank all the key stakeholders including the children of Sri Lanka who supported to make this first ever national scale study on online violence against children a success.



K.M.S.D. Jayasekara

State Secretary
State Ministry of Women and Child Development,
Pre-Schools & Primary Education,
School Infrastructure & Education Services



State Ministry of Women and Child
Development, Pre-School & Primary
Education, School Infrastructure &
Education Services

Message from SPARC

University of Colombo

The Social Policy Analysis and Research Center is the focal point of research in the Faculty of Arts of University of Colombo. Since its inception, the center has thrived to carry out international and nationally significant research with an aim to make fruitful contributions to improve the lives of Sri Lankans while contributing to the multi-disciplinary research culture in Sri Lanka.

This is another landmark study for the center; also addressing a timely need by exploring the prevalence of online violence against children in Sri Lanka. This is the first study of this nature in South Asia and the second study conducted in Asia. The findings provide a comprehensive picture of the seriousness of the issue and lobby to take immediate action to mitigate and ultimately end online violence against children.

I wish to thank the State Ministry of Women and Child Development, Pre-Schools & Primary Education, School Infrastructure & Education Services for commissioning the study and Save the Children International for selecting SPARC to conduct the study. Save the Children International provided great support to the research team to overcome research and financial challenges. I also wish to thank the Vice Chancellor of the

University of Colombo, Senior Professor Chandrika N. Wijeyaratne for the support extended in obtaining approvals enabling us to duly complete the study.

I also wish to acknowledge the exponential contribution made by Professor Wasantha Senewiratne, Mr. M.A.M Hakeem and Mr. Sampath Chandrasena as the child protection expert, leading legal consultant and cyber security expert of the study. Moreover, I would like to especially thank Mr. Malith de Silva for his efforts to complete the research outcomes in due course as a sociologist and the research coordinator.

Also, I wish to acknowledge the support extended by the Department of Probationary, District level data collection officers and specially the respondents of the study including interviewed children, key informants and national and international experts on online violence against children.

Finally, I hope this study would support policy makers and practitioners to provide a better and efficient service to the children of Sri Lanka and I hope that it would be a stepping stone for further research in the subject area.



This is another landmark study for the center and it addresses a timely need by exploring the prevalence of online violence against children in Sri Lanka



Dr. Nishara Fernando

Director
Social Policy Analysis and Research Center
Faculty of Arts
University of Colombo



Message from Save the Children International, Sri Lanka

The expanding digital environment affects children in a multitude of ways. As active users of online spaces, children explore a wide variety of platforms and material online, which expose children to many knowns and unknowns. It has become a normalized but also at times a critical part of life for many children and young people, and perhaps an equally familiar environment as the natural environment around them.

But at times more than the natural environment, the digital environment carries risks for children that should be appropriately mitigated, so that children are able to safely engage in online spaces. Online violence against children has seen a steep incline over the years, accelerated by rapid advancements in technology, increased online users and contextual dependencies on online spaces such as the COVID-19 context.

As an organisation working for the fulfillment of children's rights and the protection of children, one of the greatest obstacles that we have encountered is the absence of rigorous data and research evidence to understand the scope and scale of the impact of online violence on children. A lack of evidence makes responding to the problem effectively and impactfully, a great challenge.

Therefore this research is groundbreaking in many ways. For the first time in Sri Lanka, national data has emerged on the prevalence of online violence, and its impact on children. Furthermore, the research has unearthed significant

loopholes and barriers in service provision that needs to be addressed, paving a good foundation for advocacy.

I am very grateful for all those who worked tirelessly and over a very challenging period of time to complete a comprehensive, quality and technically sound research. Foremost, I extend my gratitude to the State Ministry of Women and Child Development, Pre-schools and Primary Education, School Infrastructure and Education Services, for collaborating with Save the Children and World Vision in commissioning this research. I deeply appreciate the dedication of the Social Policy Analysis and Research Center at the University of Colombo who led this research, in collaboration with Save the Children and World Vision. I am thankful to all the participants, especially children who have given their honest views and opinions, and shared many difficult experiences with the researchers. I sincerely acknowledge the Global Partnership to End Violence Against Children, whose funding made this research possible, and all other technical and non-technical consultants, experts and other stakeholders of both government and other sectors who supported this research in numerous ways.

This is a collective achievement; which I hope will build the foundation for many more collective and collaborative engagements towards ending online violence against children.



Therefore this research is groundbreaking in many ways. For the first time in Sri Lanka, national data has emerged on the prevalence of online violence, and its impact on children



Julian Chellappah

National Director
Save the Children International
Sri Lanka



Save the Children

Message from World Vision Lanka

Driven by the desire to make our lives easier than ever before, the digital technologies have multiplied rapidly throughout many fields in the recent years. Unfortunately, this change has also paved the way for increased cyber-violence across the world. Technology has provided abusers new methods for reaching, stalking and controlling their victims and enabled them to overcome various physical protection measures and geographical boundaries. The abuse could be a combination of online intimidation with offline abuse leading to physical violence.


While researches suggest that both adults and children are likely to be victims of online abuse, children are more vulnerable due to their age and immaturity. Children are exposed to a wider spectrum of technologically facilitated environment due to their development-oriented tasks. The digitalized learning environment that has been suddenly imposed on children due to the closure of schools as a result of the COVID-19 pandemic is such an example. The internet and technology are useful tools for children, but they also present serious safety concerns to

children unless adequately addressed at all individuals deserve protection from such abuse. Nevertheless, as it is well established that females are far more likely to be victims.

While there has been limited research on the cyber related abuse, there is a dire need to have updated research on this area. Such a gap will not make it possible for the policy makers or law enforcement authorities to take necessary precautionary measures or preventive actions to protect the millions of online users.

In such a time as this, I am happy that World Vision Lanka is able support the partnership that made it possible to conduct this special research on the incidence, nature and scope of online/ cyber violence against children in Sri Lanka and related response mechanisms. We sincerely hope that the findings would help make the necessary changes in policy and legal reforms and improve related responses, and we look forward to extending our fullest support for the same.



In such a time as this, I am happy that World Vision Lanka is able support the partnership that made it possible to conduct this special research on the incidence, nature and scope of online/ cyber violence against children in Sri Lanka and related response mechanisms 



Dr. Dhanan Senathirajah

National Director
World Vision Lanka

World Vision 

Executive Summary

Research on Incidence, Nature and Scope of Online/Cyber Violence against Children (OVAC), and the Mechanisms that Respond to Cases of Online/Cyber Violence against Children in Sri Lanka

Introduction

The digital/cyber landscape of Sri Lanka has been on a path of rapid transformation since the dawn of the new millennium, and virtually is on an accelerated growth since the beginning of the second decade of the 21st century. Contemporary studies conducted in the Asia-Pacific region, the Americas and Europe have indicated that new forms of online/cyber abuse against children are on the rise such as cyber sexual exploitation, cyber bullying and extortion, online grooming and cyber/digitally enabled extremist/violent radicalization of children, among many others. In recent sporadic studies and statistics it has become evident that those types of cyber violence have been committed against the children of Sri Lanka over the span of the last decade. However, the lack of systematic studies on the issue had been hindering the policy makers and implementers from grasping the exact nature, scope and impact of the problem. Therefore, in 2019, the Ministry of Women and Child Affairs of Sri Lanka together with Save the Children International, World Vision Lanka and LEADS (project partner organizations), commissioned this research study on the **incidence, nature and scope of online violence against children, and the mechanisms that respond to cases of online violence against children in Sri Lanka**. This research is a part of

a project supported by the GPEVAC that aims to end all forms of online violence against children in Sri Lanka.

This study has three key objectives:

- To assess the incidence, magnitude and impact of online/cyber violence against children in Sri Lanka.
- To assess the nature and effectiveness of response and support mechanisms currently available for children in responding to incidents of online/cyber violence committed against them.
- To learn and incorporate the views and proposals of children on measures required to prevent online/cyber violence, and a responsive and impactful response mechanism, that addresses both the effective and efficient enforcement of the law, as well as provision of appropriate and effective psychosocial support.

The research design and the research questions were developed in order to achieve the aforementioned three key objectives.

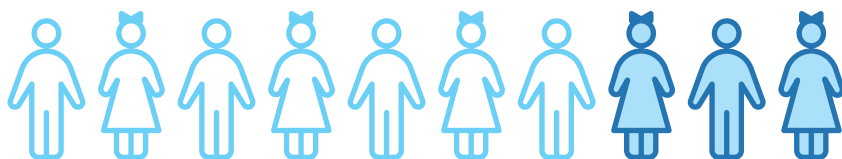
Methodology

This research employed a fusion of both quantitative and qualitative methods in order to grasp a clear picture of the issue of online/cyber violence against children in Sri Lanka. The original research design included a survey of 2,400 children

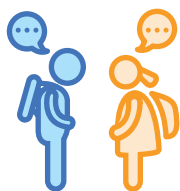
covering all 25 districts. However, due to the Covid19 pandemic this design was reformed under a contingency plan. The largest portion of the data has been derived from a quantitative, one-to-one survey conducted with 1,911 children, covering all 25 districts of Sri Lanka (965 boys; 946 girls). Other tools included focus group discussions with children, key informant interviews with children and international experts cum national/provincial level stakeholders, and an intensive context/literature review cum legal gap analysis.

The research team together with the project partner organizations ensured that in the conduct of the research that the principles of 'no harm to children' and 'in the best interest of the child' were strictly observed. In order to ensure this all the personnel involved in the research were trained in child safeguarding, and perhaps for the first time in Sri Lanka, a Guideline on Conducting Research with Children was developed under the guidance of the Technical Working Group formed by the project partner organizations. Furthermore, a Child Risk Assessment Framework, especially designed for this research by the research team and the project partner organizations had been employed. The research methodology received the approval of both the Ministry of Women and Child Affairs, and the Ethics Review Committee of the Faculty of Arts, University of Colombo.

Research on the incidence, nature and scope of online violence against children and the mechanisms that respond to cases of online violence against children.



03 out of **10** children who participated in the study have experienced some sort of online violence.



24%

of the Children who have experienced online violence had confided in a friend about their experience of online violence instead of parents, teachers or adults

More girls are victims of online violence compared to boys.



29%



27%

The Incidence, Nature and Scope of Online/Cyber Violence against Children (OVAC) in Sri Lanka

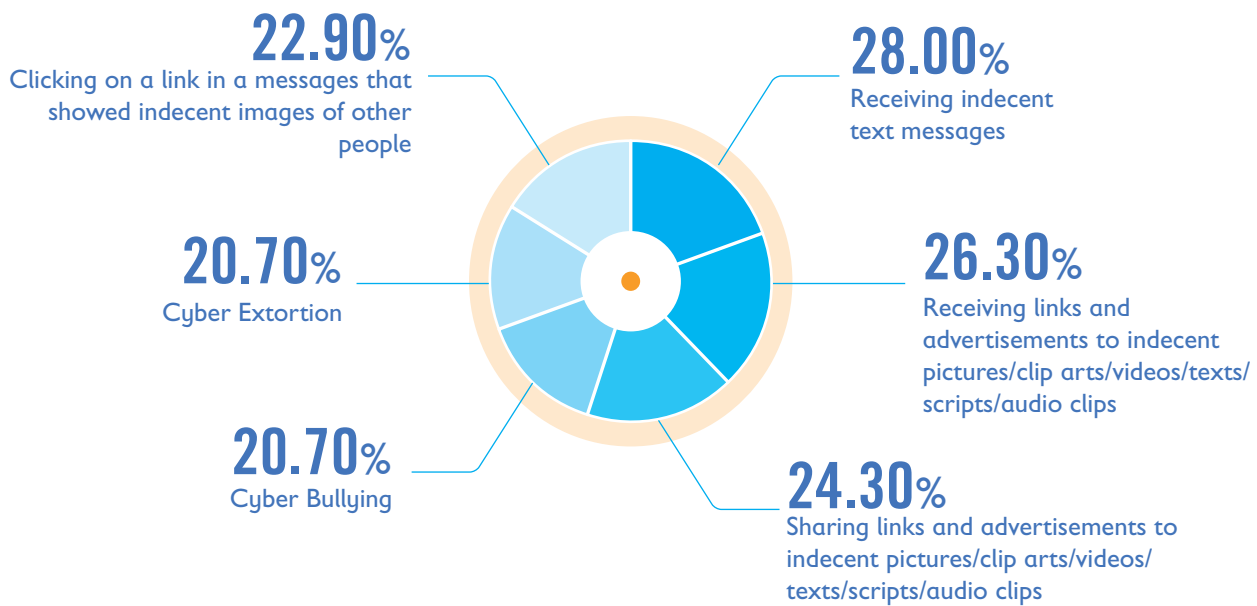
The findings of the study revealed that over 28% of children have experienced some kind of online violence. In other words, **three out of every ten children** interviewed in the study have experienced some sort of online violence. Girls (29%) have suffered slightly more from online violence compared to boys (27%). These instances of online violence include receiving an indecent message (28%), receiving indecent links and advertisements 26% and having an indecent link/message being shared in a group. In addition, 27% of children have experienced cyber bullying and extortion, while nearly 20% have had an indecent image of them being shared on the internet. The findings suggest a significant prevalence of online violence against children in Sri Lanka.

Of the children who have experienced online violence the most have experienced any form of online violence while using Facebook (Boys – Nearly 74% / Girls – nearly 58%), Instagram (Boys – nearly 41% / Girls – Nearly 52%) and Twitter (Boys – 25%/ Girls- Nearly 41%). This indicates that children using any social media platforms are vulnerable to online violence. Children are more likely to share an experience of online violence with a peer than an adult, as a significant portion (over 24%) of children who have experienced violence had confided in a friend around their own age about the incident. The children had rarely informed an adult about an instance of online violence and children identified that the generation gap and being afraid of being further victimized by adults deter them from revealing the experience of online violence to adults. A significant number (61) of children who had experienced online violence stated that they were too scared to complain to an authority. Twenty five children stated

they were threatened with revealing their personal information if they reported to authorities. Sixteen children stated that their lives were threatened. Another fourteen children stated they were given gifts to keep the online violence as a secret.

The children and the key informants identified characteristics that make children vulnerable to online violence. The gender of the child might be an important characteristic, as the finding revealed that girls have a slightly higher tendency to experience online violence than boys. Another characteristic was lack of parental supervision. Children and key informants agreed that lack of parental supervision allows perpetrators to exploit children. Moreover, sharing personal data and pictures publicly was also seen as a characteristic. Children felt that sharing this information publicly could lead to online violence such as edited pictures and identity theft.

Types of Online Violence



Children identified the impacts of online violence to be interrelated and complex. The key impacts identified by children include isolation from family and peers due to shock and shame, decreased academic performance, mental health issues and behavioural changes. The level of impact of online violence varies according to subjective factors such as the personality of children, family background and support available to children at home and schools.

Awareness of Online/ Cyber Violence

Children stated that the majority of parents (73%) find it difficult to supervise children's internet use because they lack knowledge of how the internet works and in which ways children can be exposed to online violence. They added that parents also lack an understanding of how to take legal measures when children experience online violence (69%) and

that the majority of the children stated they would not confide in a parent if they experience online violence. Moreover, ninety five percent of children believe educators have awareness about online violence. However, children stated that they would not confide in an educator, because:

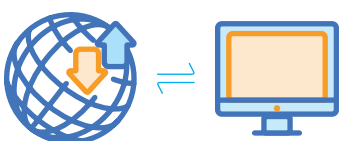
- (1) educators often blame the child for the online violence (67%),
- (2) educators do not protect children's confidentiality and privacy (19%),



73% of parents find it difficult to supervise children's use of internet as they lack awareness of how the internet works and how children can be exposed online violence against children.

Characteristics that make children vulnerable to online violence.

- Trusting people you meet in online platforms too much
- Sharing personal information publicly on social media platforms.
- Lack of awareness of online violence
- Lack of supervision by parents



71% of children stated that internet service providers do not have a good understanding of online violence as they do very little to curb online violence. The key informants added to this criticism on two grounds; one is that the ISPs have failed to take responsibility for the internet service they provide, and secondly the ISPs' lack of support to law enforcement authorities.

- (3) nearly 10% of children stated that educators would create issues at school, and, finally,
- (4) nearly 9% said they are afraid of their teachers.

Over 71% of children stated that internet service providers do not have a good understanding of online violence, as they do very little to curb online violence. The key informants added to the criticism on two grounds: one is that the ISPs have failed to take responsibility for the safety of the internet service they provide, and secondly the ISPs' lack of support to law enforcement for crimes committed using their services.

The Role of Mass Media —

Children also commented on the role of mass media in the battle against online violence. Over eighty four percent of children stated that Sri Lankan mass media is aware of online violence. Nearly

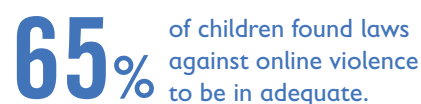
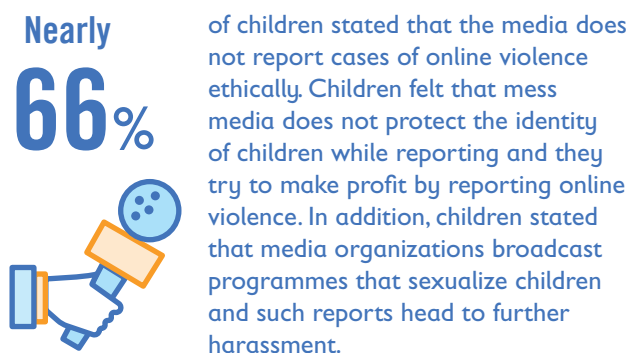
sixty six percent of children (1,254) stated that media do not report cases of online violence ethically. According to the children, a number of factors point to irresponsible reporting on the subject of online violence. Nearly 64% of children stated mass media organizations do not protect the identity of children while reporting and nearly 10% stated that media organizations try to make a profit by reporting online violence. Moreover, more than 4% of children stated that media organizations broadcast programmes that sexualize children and another 4% stated that media reports sometimes lead to cyber bullying and further harm to victimized children.

Views of the Children Regarding the Existing Legal Mechanisms —

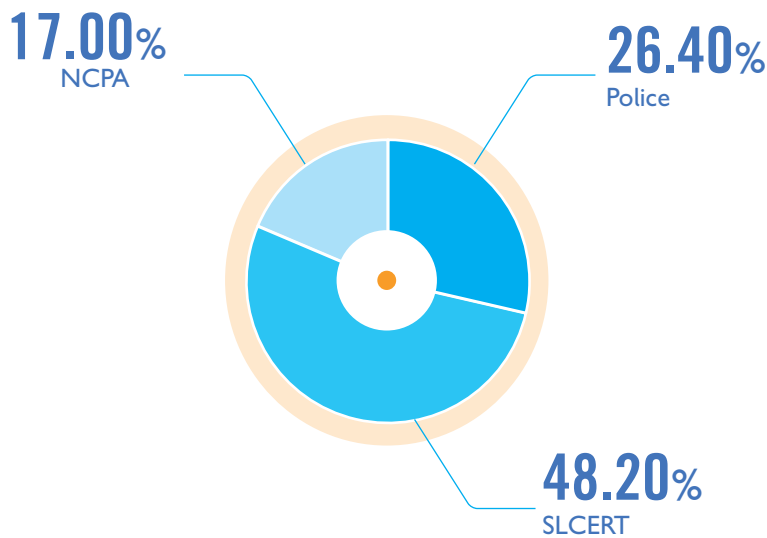
The study also explored the legal dimension of online violence against children in Sri Lanka. Findings suggest

that the majority of children (65%) found the existing laws against online violence to be inadequate and to require further improvements. The key informants also agreed with the premise and suggested amending existing law to directly address online violence. Due to the inadequacy of law and efficient legal procedures, 92% of children stated that they would not seek legal support when faced with online violence. They also identified other factors that deter children from seeking legal support, such as:

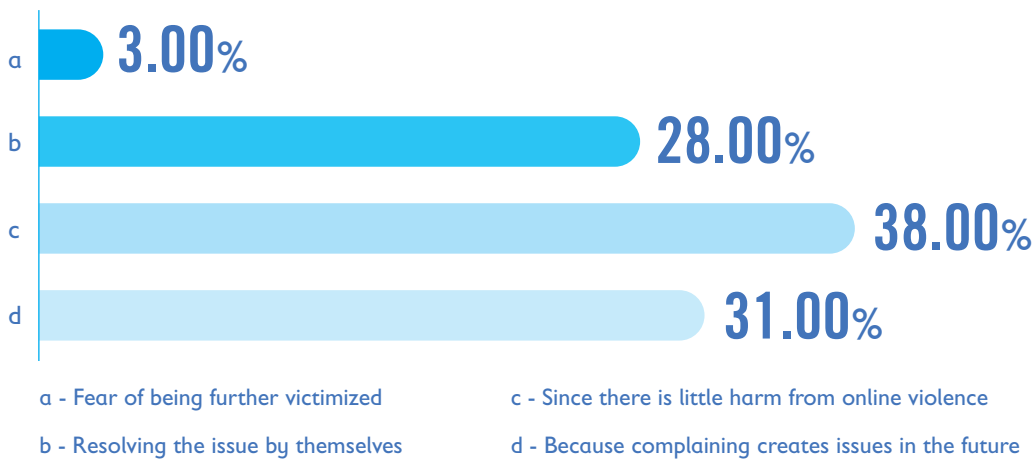
- (1) the fact that they consider online violence to be less of a harm (38%) than violence in the “real” world,
- (2) because legal procedures related to online violence take a long time to resolve (31%),
- (3) because children often try to resolve the issues by themselves (28%) and
- (4) due to fear of the perpetrator (3%).



Complaining to Legal Authorities



Reasons for Not Seeking Legal Support



Existing Technology-driven Response Mechanisms

In addition to the sociological and legal dimensions, the study explored the cyber security dimension of online violence against children. The findings revealed that Sri Lanka needs to take new and robust action to curb online violence. The key informants suggested that open source software can be utilized

to track down Child Sexual Abuse Material (CSAM). The study noted that the National Child Protection Authority (NCPA) has taken many steps to improve child safety online, including establishing a cybercrime unit to fight OVAC and introducing a CSAM reporting helpline, etc. However, further improvement has to be made to respond to OVAC efficiently and effectively.

Recommendations

Policy Reforms and Civic Awareness

The findings of the study reveal that online violence against children has become a serious issue in Sri Lanka. In this light, the study recommends the adoption of multiple measures to mitigate and eradicate online violence against children in Sri Lanka. These include a proposal for reform of the national education curriculum to introduce lessons on online violence as a subject in Civic Studies courses from Grade 09 at least up-to GCE O/L, introducing new online awareness raising programmes, increasing the awareness of parents and increasing the sensitivity of educators when handling cases of online violence.

Legal Reforms

In addition, to rectify the gaps in the legal system, the research team recommends that: 1) the Sustainable Development Council of Sri Lanka (SDCSL) formulate relevant state policies and amend the SDG targets related to OVAC to include a specific section on OVAC to the National Policy on Child Protection (NCPA, October 2019) that establishes a uniform system and structure and coordination among the relevant agencies and authorities, 2) a harmonization of terminology used to address OVAC, 3) adopting the Budapest Convention on Cybercrime (the first international treaty seeking to address internet and computer crime by harmonizing national laws, improving investigative techniques, and increasing cooperation among nations),

4) disseminating Conventions and Agreements or national policies on OVAC to all the levels of implementation authorities. Furthermore, the team recommends that the Sri Lanka Computer Emergency Readiness Team (SLCERT), the focal point for cyber-security in Sri Lanka, introduce systematic categorization of their complaints by age and gender, introducing hard law instruments to protect child victims, technical and legal revision of Penal Code sections: 286A, 286B, 288A, 288B, 308, 308A, 360B, 360C, 365, 365A and 365B, 368. Many of the changes needed to protect Sri Lankan children online would come from implementing the recommendations made in The National Plan of Action for Children in Sri Lanka (2016-2020) and by incorporating offences related to child pornography, the commercial sexual exploitation of children, cyber-entertainment, online grooming, cyber-sexual harassment, cyber bullying and cyber-stalking in the Penal Code or Computer Crimes Act as offences connected to OVAC. As with any criminal child abuse or neglect, parents, guardians, caregivers, principals and teachers or any other adults who have knowledge of OVAC and failed to protect children from it, should be made criminally responsible for non-disclosure of the information and educating stakeholders involved in matters relating to the welfare and best interest of the child about OVAC. Finally, child welfare stakeholders must be educated about OVAC, along with ways to protect against it and to report it when it occurs.

Technology-driven Solutions

Though the problem of online violence is rooted in technology, there are increasingly technology solutions that can help to address it. The research team recommends international training opportunities for NCPA employees, establishing a ticketing system to track complaints reported to the NCPA, providing secure and dedicated hardware and internet connections to the cyber-crime unit of NCPA, upgrading the investigation methods used by the cyber-crime unit, initiating collaborations with international organizations dedicated to fighting online violence against children, collaboration between the NCPA and the Telecommunications Regulatory Commission of Sri Lanka (TRCSL) and the introduction of new regulations to legally require ISPs to support authorities by obtaining phone records and internet usage histories more efficiently.

Cross-Sector Partnerships

Most importantly, this study highlights that creating and scaling up the necessary solutions to put an end to online violence against children will require much greater, and much more effective, collaboration across sectors of society than has been seen before. Cross sector partnerships, involving more actors from government, business/industries, civil society, UN agencies and/or other non-state actors (such as academia), is crucial.

Chapter 01

Introduction

The **‘Research on the Incidence, Nature and Scope of Online/Cyber Violence against Children (OVAC), and the Mechanisms that Respond to Cases of Online/Cyber Violence against Children in Sri Lanka’** was commissioned by the Ministry of Women and Child Affairs (the predecessor to the State Ministry of Women and Child Development, Pre-schools and Primary Education, School Infrastructure and Education Services) under the technical support and leadership of Save the Children and World Vision Lanka in 2019. This research was conducted by the Social Policy Analysis and Research Centre (SPARC) of the University of Colombo.

This national study – the first of its kind in Sri Lanka, and one of the pioneering researches in South Asia regarding the scope of online/cyber violence against children was launched with the support of the Global Partnership to End Violence Against Children (GPEVAC) in order to address a major deficit of knowledge regarding the magnitude of online/ cyber violence experienced by the children in Sri Lanka. As a country that has been experiencing a rapid growth in the ICT sector over the last two decades, Sri Lanka has seen numerous cases of online violence committed against its children. However, the scarcity of evidence, knowledge and information regarding the issue hindered the key stakeholders from addressing it effectively.

Therefore this study had three key objectives; and the research design and the research questions were developed in order to achieve those objectives given below:

- To assess the incidence, magnitude and impact of online/cyber violence against children in Sri Lanka.
- To assess the nature and effectiveness of response and support mechanisms currently available for children in responding to incidents of online/cyber violence committed against them.
- To learn and incorporate the views and proposals of children on measures required to prevent online/ cyber violence, and a responsive and impactful response mechanism, that addresses both the effective and efficient enforcement of the law, as well as provision of appropriate and effective psychosocial support.

Despite the challenges posed by the Covi19 pandemic the research team was able to successfully complete the study with the immense support of the Technical Working Group led by Save the Children International. This study included a survey of 1,911 children covering all 25 districts of Sri Lanka representing urban, semi-urban and estate settlements. The research team also conducted focus group discussions with children at district level and key informant interviews at provincial, national and international levels with key

stakeholders and experts in the fields of child protection, law enforcement and IT industry.

Through this research, the children of Sri Lanka have voiced up their experiences and views pertaining to online/cyber violence. This report has summarized all the key findings of the study. Chapter two of the report presents a brief context review on OVAC, then followed by a discussion of research’s methodology in chapter three. Chapter four provides all the key findings of the research, and is followed by chapter five briefly outlining the legal gaps pertaining to OVAC in Sri Lanka, and chapter six outlining the tech-driven avenues to tackle OVAC available for Sri Lanka. Chapter seven discusses in detail the recommendations of the research, a majority of which was enunciated by the participant children. In conclusion, this report sign-posts towards possible future researches and developments identified through the study.

Chapter 02

Context Review

2.1 Cyber-space: A New Spatial Realm

The 'internet' or in a broader sense the 'cyber-space' is perhaps one of the most complex human inventions of the 20th century, and it only keeps growing at a rapid rate in the 21st century. The 'internet' or the 'cyber-space' has become another spatial realm in which a plethora of human activities take place from education to entertainment; from financial activities to crimes/violence. It transcends physical boundaries and no longer coterminous with the physical human geography. This inherent nature of the cyber-space makes it extremely difficult to address the forms of violence which take place within by any single sovereign state alone. The crimes and violence that take place within the cyber-space are underpinned by an economy of 'demand and supply' by perpetrators who do not have to commute across physical boundaries to achieve their gratification. This complex nature of the cyber-space as a 'new spatial realm' requires a concerted global effort to regulate, investigate, govern and prevent the harmful activities that take place within it.

2.2 Cyber-space and Children: The Dangers

Today's children across the globe are much sharper with handling technology than it was the case forty years ago. The Global Threat Assessment Report (2019) informs that within a year 122 million more children have become users of the internet/cyber-space. The rapid growth of the IT industry has made the 'cyber-space' or the 'internet' a household commodity. It no longer requires a desktop or a laptop to be connected to the internet; the rapid development of the mobile telecommunications industry has now made it only a matter of moving one's finger tips to access the internet/cyber-space. While the cyber-space had a multitude of benefits for children in the forms of education, arts, entertainment and communication, it also exposes them to severe life altering harm.

The Global Threat Assessment Report (GTA 2019) published by the WeProtect Global Alliance identified that there is an expanding sphere of harm which is exceeding – at a rapid rate – the capacities of responsible authorities to tackle and reduce online violence against children (OVAC). It further identified four key elements that converge together to increase the level of harm experienced by children, especially the online commercial sexual exploitation of children (OCSE). The four elements are:

- (i) Global Technology Trends
- (ii) Rapidly changing offender behaviour
- (iii) Victim's online exposure
- (iv) Socio-environmental context

2.2.1 Global Technology Trends

There is a rapid increase of perpetrators who are opting to use Dark Web due to recent technological advancement. They do so to share child sexual abuse material (CSAM) and tips for grooming of children, and evading detection. In addition to the increase of Surface Web Services which allow for greater privacy, security and anonymity, there is a rise of encryption. These services include secure P2P file-sharing networks, hosting services, mobile payment methods and messaging services that bypass the need for registration and identification. Thus the current global trends in technology are lowering the barriers to entry for perpetrators and CSAM/OCSE.

2.2.2 Rapidly Changing Offender Behaviour

There is a dire lack of understanding about the behavioural patterns of the perpetrators and this demands more systematic studies to comprehend the behaviour, objectives, and forums used by the perpetrators. As the GTA 2019 pointed out, over a period of nearly twelve months, there had been a 100% increase in the CSAM material reported by tech companies; and a 33% increase in the removal of URLs containing CSAM by the Internet Watch Foundation

(IWF). What has been understood of the offenders can be summarized as;

- (a) not all offenders are paedophiles;
- (b) negative or adverse conditions in early development can contribute to their behaviour;
- (c) while visible offenders come from across the globe and all walks of life, a majority are ethnic Whites. However, these data is only about the 'visible offenders' and there is a scarcity in the understanding regarding the 'invisible offenders', the ones that go un-noticed.

2.2.3 Victim's Online Exposure

With the age at which children access to devices and unsupervised access to social media and online gaming reducing each year, they are becoming more vulnerable to online violence. Normalization of risky online behaviours overtime has resulted in a large number of children sharing self-generated sexual content. This has increased the volume of material available to offenders and increases children's vulnerability to exploitation and abuse by adult perpetrators. It is also alarming to see the rise of numbers of children who participate in forms of cyber/online violence against their peers.

2.2.4 Socio-environmental Context

According to the GTA 2019, over 367 million new internet users have appeared over a period of 12 months. Most of these new users are from developing countries or the Global South who do not have sufficient/adequate protection, prevention and response mechanisms to cope with the negative impacts of internet/cyber-space. The report has also noted that children ranging from infants to late adolescents are susceptible to online violence in these developing countries or the Global South. Especially in lower income regions, children are at a greater risk of being commercially exploited online to provide income for their families.

2.3 Children of Sri Lanka and Online Violence

Sri Lanka has experienced a rise of internet use and home broadband connections over the past decade, and internet connections had increased by 20% in 2017 (Razak, 2018). The study conducted by the UNICEF and IPID (2017), Sri Lankan children access the internet at an average age of 13 years. One can infer that, in line with the global trends, Sri Lankan children are exposed to online harm as well. However, until now, there had been only a limited understanding regarding the incidence, nature and scope of online/cyber violence against children in Sri Lanka due to lack of systematic studies.

The alternative report published by PEaCE/ECPAT Sri Lanka (2017) revealed that foreign child sex offenders have produced CSAM involving Sri Lankan children and these materials have been on circulation. The aforementioned study by the UNICEF/IPID (2017) revealed some risky behaviours on the part of children such as sharing information with unknown persons online, refusal to change their privacy settings, lack of knowledge regarding support systems and legal authorities, and real-life/offline meetings with the persons whom they communicated through online means.

In 2019, the National Child Protection Authority of Sri Lanka established a special Cyber-Crime/Surveillance Unit to respond to OVAC effectively and efficiently. This initiative has been further strengthened by the launch of a child friendly mobile application to report incidents of online and offline violence against children.

It is imperative that the findings of this 'Research on Incidence, Nature and Scope of Online/Cyber Violence against Children in Sri Lanka' will contribute to enhance the aforementioned initiatives of the NCPA and other organizations that work towards the well-being and protection of the children of Sri Lanka. The next chapter of this research shall detail out the methodology utilized for this research.

Chapter 03

Research Methodology

As a research conducted with children on a highly sensitive subject matter, the research team in collaboration with the project partner organizations spent a considerable time and thorough attention in developing the research methodology. It was imperative to ensure that while the research design had been tailored for effectiveness and efficiency that the entire design met the ethical parameters and would cause no harm to participant children through the conduct of this research.

Data Collection

Both Primary and Secondary data as well as qualitative and quantitative data was collected from research locations. To achieve the mentioned objectives, the research team developed a research design comprising of components discussed in the following section. The research design was submitted to the Ministry of Women and Child Affairs (the predecessor of the State Ministry of Women and Child Development) for approval.

The research team followed research ethics rigorously starting with the research design. In addition to obtaining the approval from the ministry, approval was also gained from the Ethics Review Committee of the University of Colombo, Faculty of Arts for the research methodology. Moreover, the research team followed a strict selection criteria when selecting enumerators to collect data from children. The enumerators were asked to produce character certificate from the respective Grama Niladari office. After initial screening the enumerators were given a two day residential training on data collection tools, code of conduct when collecting data from children, managing issues that arises in the field etc.

Review of secondary data

The study consists a literature review of existing studies, reports and key policy and strategy documents to understand the global and local context on online violence, abuse and exploitation

impacting children, including issues related to violent content, hateful, damaging or otherwise harmful material, child sexual abuse material (CSAM), inappropriate contact, online grooming, exploitation and trafficking, cyber-sexual harassment of a child, self-exposure, Children's involvement in cyber-crime and other concerns.

As a part of the review of secondary data the research team developed a glossary of terms to be used in the study. The research team used the terminology proposed in the "Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse" issued by the Luxembourg guidelines.

Child: "for the purposes of the present study, a child means every human being below the age of eighteen years unless under the law applicable to the child, majority is attained earlier." For the purpose of this study, only the children aged between 13 to 17 years were participated.

1. **Online child sexual exploitation:** "all acts of a sexually exploitative nature carried out against a child that have, at some stage, a connection to the online environment"
2. **Child sexual abuse material:** material depicting acts of sexual abuse and/or focusing on the genitalia of the child.
3. **Self-generated sexual content:** "the material or content is self-generated (whether illegal or not, and whether coerced or not); sexualised (but leaving aside indecent, which may involve a more subjective value judgement); and involving children".
4. **Exposure to harmful content:** to children accessing or being exposed to, intentionally or incidentally, age-inappropriate sexual or violent content, or content otherwise considered harmful to their development.
5. **Live streaming of child sexual abuse:** sexual abuse transmitted to viewers through "streaming" over the Internet.

6. **Grooming/online grooming:** the process of establishing/building a relationship with a child either in person or through the use of the Internet or other digital technologies to facilitate either online or offline sexual contact with that person.
7. **Sexual Extortion:** blackmailing of a child with the help of self-generated images of that child in order to extort sexual favours, money, or other benefits from her/him under the threat of sharing the material beyond the consent of the depicted child.
8. **Sexual Harassment of children:** refers not only to sexual conduct with the explicit intention to violate the dignity of another child (i.e. purpose) but also to conduct of a sexual nature that a child experiences as offensive or intimidating.

Data Collection Techniques – Children using internet

The research team utilized multiple data collection tools when collecting data from children including a structured questionnaire and in-depth interviews. After much deliberation the research team decided to conduct the data collection activities at the household level taking the volatile situation caused by Easter attacks and the spread of COVID – 19 virus in the country in the data collection period. The initial drafts of instruments were developed in English and were subsequently translated to Sinhala and Tamil languages after obtaining the due approval from the Technical Working Group (TWG) led by Save the Children and World Vision Lanka.

(a) Semi – structured questionnaire with children using internet

A semi-structured questionnaire was carried out with the selected sample of children who use internet. The questionnaire included open and close ended questions that covers dimensions including prevalence, nature, magnitude,

knowledge and impact of different types of online violence against children.

Further it included questions tailor made to identify characteristics of children's online behaviour, motives and causal factors that lead to online violence, factors that make children vulnerable to online violence, awareness of children on the rights relating to online violence, response mechanisms and avenues of support available to them in the event of victimization, if they already have sought out support then the nature of their experience, reasons for non- engagement, nature of support children require to prevent online violence and types of prevention strategies children prefer; and key components and strategies that should be included in an effective prevention and response mechanism.

The research team refrained from directly asking sensitive questions from the children when conducting questionnaires in households. These sensitive questions are experiences of online abuse, forms of abuse children have experienced online etc. Hence, a special short questionnaire was administered to the children containing the most sensitive questions. The children were then asked to provide answers to these questions on their own. Once the questionnaire was filled the data collection officer sealed the short questionnaire in an envelope which was then attached to the main questionnaire.

(b) Focus group discussion with children

Focus group discussions were carried out with children to primarily collect in-depth data on the subject matter, as well as to validate and verify the data collected using the questionnaire and the key informant interviews. An interview schedule was developed which included open ended questions that aimed to comprehend prevalence, nature, magnitude, knowledge and impact of different types of online violence against children, and attitudes and practices of educators (principals, teachers, counsellors etc.), parents and caregivers/children (girls and boys) from the children's point of view.

In addition, it included questions that focused on characteristics of children's online behaviour, motives and causal factors that lead to online violence, factors that make children vulnerable to online violence, awareness of children on the rights relating to online violence, response mechanisms and avenues of support available to them in the event of victimization. Furthermore it also investigated if they have sought out support, nature of their experience in receiving support, reasons for non- engagement, nature of support children require to prevent online violence and types of prevention strategies children prefer, as well as, key components and strategies that should be included in an effective prevention and response mechanism.

Provincial Key informant interviews with relevant stakeholders using a semi-structured interview schedule

Key informant interviews were carried out using a semi-structured questionnaire with purposively selected stakeholders including parents and care givers, principals, teachers, counsellors, clergy, government officials responsible for protection, care and development of children including Child Rights Promotion Officer, Education officer, Probation Officer etc.

The semi-structured interview schedule was developed with open ended questions that focused on prevalence, nature, magnitude, knowledge and impact of different types of online violence against children, attitudes and practices of educators (principals, teachers, counsellors etc.), parents and caregivers/children (girls and boys). In addition, it included questions that focused on characteristics of children's online behaviour, motives and causal factors that lead to online violence, factors that make children vulnerable to online violence, awareness of children on the rights relating to online violence, response mechanisms and avenues of support available to them in the event of victimization. Furthermore the interviews also investigated if children already

have sought out support, the nature of their experience in receiving support, reasons for non- engagement, nature of support children require to prevent online violence and types of prevention strategies children prefer, as well as key components and strategies that should be included in an effective prevention and response mechanism.

Key informant interviews with National and International Level Experts and Stakeholders

In addition to the above mentioned techniques expert interviews were carried out with experts on child protection, human rights, cyber- security etc. who are employed or partners of government agencies, non-governmental organizations and international organizations.

An interview schedule was developed which included open ended questions that aimed to comprehend the current legal, policy and institutional/ administrative frameworks, interventions and services available for the protection of child victims of online violence, current policy, legal and institutional/ administrative frameworks that apply to prevent online violence against children, effectiveness of the past and current strategies to prevent and respond to online violence against children, and the key components and strategies that should be included in an effective prevention and response mechanism.

Sample Selection

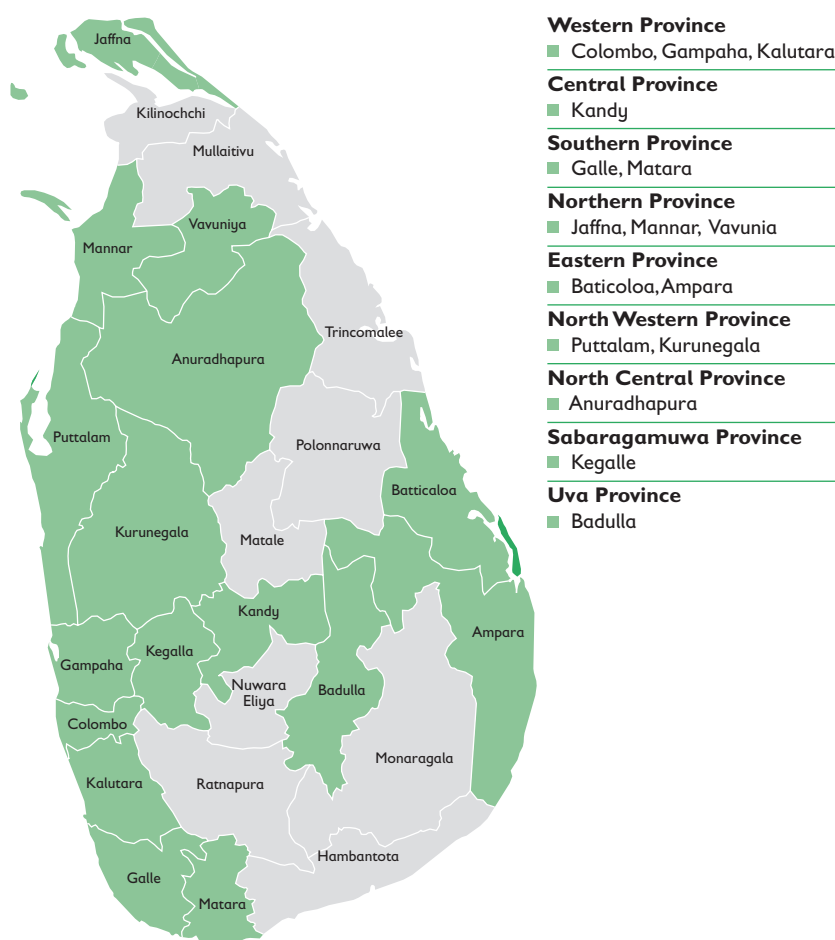
Original Sample frame of the Survey

2012 housing and population census was used as the sample frame of the survey. According to the 2012 housing and population census the total population in Sri Lanka was 20,359,439. Out of total population 18.2 percent lived in urban sector, 77.4 percent were living in rural sector and only 4.4 percent lived in the estate sector. Initially it was decided to conduct 96 questionnaires with children (between the ages of 13 to 17 years) from each district which would amass a sample of 2,400. The sample was to be selected from Urban, Rural and Estate sectors.

District	Urban	Rural	Estate	Total
1. Colombo	75	21		96
2. Gampaha	15	81		96
3. Kalutara	15	81		96
4. Kandy	11	78	6	95
5. Matale	11	81	4	96
6. Nuwara Eliya	6	39	51	96
7. Galle	14	82		96
8. Matara	13	83		96
9. Hambantota		96		96
10. Jaffna	19	77		96
11. Mannar	23	73		96
12. Vavuniya	19	77		96
13. Mullaitivu		96		96
14. Kilinochchi		96		96
15. Batticaloa	27	69		96
16. Ampara	22	74		96
17. TrincoBoyse	22	74		96
18. Kurunagala		96		96
19. Puttalam		96		96
20. Anuradhapura		96		96
21. Polonnaruwa		96		96
22. Badulla		96		96
23. Monaragala		96		96
24. Rathnapura		96		96
25. Kagalle		96		96
Total	293	2,045	62	2,400

Covid 19 Pandemic and the Contingency Plan

Unfortunately due to the rapid spread of the Covid19 Pandemic the research team in collaboration with the Technical Working Group decided to revise the sample size, and decided to resume data collection activities in two phases. In phase 1 research team focused on collecting 100 questionnaires from 16 priority districts. The 16 districts with the highest internet/digital penetration of Sri Lanka was selected as the priority districts. Internet penetration can be defined as the percentage of the internet users in a given country/region against its total population. The research team used the data emanating from the Computer Literacy Statistics 2018 published by the Department of Census and Statistics (Sri Lanka) and the Sri Lanka Annual Report published by 'We are Social'. The priority districts were:



In phase 2 data collection activities were resumed in the remaining 9 districts. However again the research team was forced to halt data collection activities due to the spread of Covid19 pandemic and as the situation escalated the research team and members of the Technical Working Group agreed to stop data collection activities and to use collected questionnaires for the analysis.

Sample selection for Expert Key Informant Interviews (EKI)

The sample for the EKI interviews was selected using the purposive sampling method. These key informants and experts represent various dimensions of child protection such as child wellbeing, law enforcement agencies, child protection agencies, child rights protection, and industry and technology sector.

The key informants and experts represented the organizations/institutions such the National Child Protection Authority (NCPA), Cyber-Crime Unit of the NCPA, Department of Probation and Child Care Services (DPCCS), National Children's Council/Children's Secretariat, Department of ICT Education – Ministry of Education, Children and Women Bureau – Sri Lanka Police, NPEVAC – Sri Lanka, LEADS, World Vision Lanka, Save the Children, Crimes Against Children Research Centre – USA, Unicef Innocenti – Global Kids Online, Sarvodaya – Fusion, Grassrooted Trust, PEaCE(ECPAT), INTERPOL, Internet Watch Foundation (IWF), and Mobitel Sri Lanka.

Analysis

Data which was collected were coded into key thematic areas which are mentioned below;

- Prevalence of online violence against children in Sri Lanka
- Help seeking behavior
- Characteristics that make children vulnerable
- Nature of impact
- Awareness of key stakeholders
- Prevention and adequacy of existing laws and support mechanisms

After thematic categorization, the data was further divided into sub themes which were identified from the primary data set. The thematic areas were then analyzed using the thematic analysis technique.

Ethical Considerations: Doing Research with Children

As mentioned at the start of this chapter, this was a research revolving around a highly sensitive topic; and it was equally sensitive as the key participants were children between the ages of 13 to 17 years old. As the research had been intended to bring out the voices of the Sri Lankan children regarding their experiences of online/cyber violence, and their views regarding the existing support mechanisms, it was imperative

that this research should be a safe vehicle for the children to enunciate themselves. Therefore the research team and the Technical Working Group took steps through the implementation of following actions:

(a) Training on Child Safeguarding

As the lead among the partner organizations, Save the Children took steps to provide a through training on child safeguarding to all the personnel involved with this research. This included a two day residential training, and various other online and offline trainings. No enumerator or research staff member was allowed to conduct interviews with children sans this compulsory training.

(b) Child Friendly Language in Research Instruments

As mentioned earlier in this chapter the research team and the members of the TWG spent a great amount of time to restructure the language and terminology used in the instruments/ tools and the delivery methods to make sure that they are child friendly. The support from the Global Kids Online in drafting the research instruments/tools was immensely helpful.

(c) Guidelines on Conducting Research with Children

One of the seminal deliverables of this research was the drafting of 'Guidelines on Conducting Research with Children', perhaps the first of its kind in Sri Lanka. These guidelines were drafted by the TWG under the aegis of Save the Children. These guidelines were drafted based on the child safeguarding policy of SCL, child safeguarding guidelines of SPARC and UNICEF recommendations on conducting research with children.

These guidelines are based on the principles of 'no harm to children' and 'the best interest of the child'. Based on these guidelines, the enumerators were advised to conduct the interviews with children at a safe physical space – homes of children – at a place in which the parents/ guardians of the children can see both the researcher and the child, but would

not interfere in the privacy and right of the child to enunciate. Furthermore, as mentioned earlier, the most sensitive questions of the research were given in a 'self-administered short questionnaire' (See Appendix 2) by which the child was allowed to express themselves in writing free of interference.

Should a child wished to exit themselves from the research, they were allowed to do so at their will. During the aforementioned trainings, the enumerators were trained to identify the signs of non-verbal communication by children. This was done to ensure that as some children, while requiring to exit the research, might not express such in verbally but would indicate through indirect body language.

(d) Child Safeguarding Risk Assessment Framework (CSRAF)

Another key deliverable of this research was the implementation of a Child Safeguarding Risk Assessment Framework (CSRAF) pertaining to the research. The SPARC had appointed one of its team members – a seasoned legal professional – as the Child Safeguarding Focal Point (CSFP) for the research. The CSRAF was developed under the leadership of the aforementioned CSFP with the support of the Child Protection Experts of Save the Children/ World Vision/LEADS and other members of the research team.

This was a referral mechanism developed in response to presumed scenarios that could arise during the conduct of data collection. These scenarios included but not limited to – misconduct towards children by members of the research team/ enumerators during the study period, a disclosure of a child abuse incident by a child/adult and/or a request for support by a child. The scenarios were categorized rationally based on the severity – general to immediate danger to life. The CSRAF was based on the shared collective social responsibility towards children by all the parties involved in the research. The detailed CSRAF is given at Appendix 3 of this report.

Limitations of the Study —

The Covid19 pandemic, as mentioned elsewhere in this research, posed significant limitations upon this research. Although it was originally planned to conduct a research with a sample of 2,400 children, this had to be limited to 1,911 children in total. Furthermore, as a result of this situation, the research team had to shift FGDs from offline settings to online platforms. Conducting FGDs on online/cyber/digital platforms was a challenge due to two reasons: children were taking part directly from their homes as individuals and were not engaging in enough in comparison to offline settings; and some children who were taking part in online FGDs under the guidance of CRPOs tended to provide ready-made answers rather than freely expressing themselves.

Another challenge in conducting this research was the cultural peculiarities in Sri Lanka. It was experienced by a considerable number of enumerators that some parents did not provide the privacy required by the child to enunciate themselves. In such instances where in the parents interfered in filling the questionnaire, the research team had to discard those questionnaires and to select a new household to conduct interview anew. The Child Protection and Participation Team of World Vision Lanka conducted a special training for the enumerators on the ways by which they could address this situation.

Chapter 04

Findings: Incidence, Nature and Scope of Online Violence against Children in Sri Lanka

The findings presented in this section emanated from the nation-wide survey and focus group discussions conducted with children in Sri Lanka, and the key informant interviews conducted with international and national experts, and national and provincial level stakeholders. The findings of this section are presented in a manner to address the following key objectives of the research.

- The incidence, magnitude, and impact of online violence against children.
- The nature and effectiveness of response and support mechanisms currently available to child victims of online violence.

Demographic data

The following section elaborates demographic data of children who completed the questionnaire in each district. It details the gender, age, ethnicity, religion, activity status and education of children.

Table 4.1 Gender

Gender	Frequency	Percentage
Boys	965	50.5
Girls	946	49.5
Total	1,911	100.0

Source: Survey Data 2020

Nearly fifty one percent (965) of children were boys while girls make up nearly forty eight (946) percent of children.

Table 4.2 Age by Gender

Age (years)	Gender		Total
	Boys	Girls	
14	160	109	269
	16.6%	11.5%	14.1%
15	329	299	628
	34.1%	31.6%	32.9%
16	245	236	481
	25.4%	24.9%	25.2%
17	231	302	533
	23.9%	31.9%	27.9%
Total	965	946	1,911
	100.0%	100.0%	100.0%

Source: Survey Data 2020

Nearly thirty three percent (628) of children are fifteen years and nearly twenty eight percent (533) are seventeen years. In addition over twenty five percent (481) are sixteen years while over fourteen percent (269) are fourteen years.

Table 4.3 Activity Status by Gender

Age (years)	Gender		Total
	Boys	Girls	
Schooling	550	637	1,187
	57.0%	67.3%	62.1%
Vocational Training	398	302	700
	41.2%	31.9%	36.6%
Currently Staying at home	17	7	24
	1.8%	0.7%	1.3%
Total	965	946	1,911
	100.0%	100.0%	100.0%

Source: Survey Data 2020

Over sixty two percent (1,187) of children were schooling. In addition, nearly thirty seven percent of children are following vocational training programmes and one percent (24) of children stay at home.

Table 4.4 Ethnicity by Gender

Ethnicity	Gender		Total
	Boys	Girls	
Sinhalese	623	550	1,173
	64.6%	58.1%	61.4%
Sri Lankan Tamil	202	254	456
	20.9%	26.8%	23.9%
Up country Tamil	34	39	73
	3.5%	4.1%	3.8%
Muslim	105	97	202
	10.9%	10.3%	10.6%
Burgher	1	6	7
	0.1%	0.6%	0.4%
	965	946	1,911
	100.0%	100.0%	100.0%

Source: Survey Data 2020

Over sixty one percent (1,173) of children are Sinhalese while nearly twenty four percent (456) of children are Sri Lanka Tamils. In addition, nearly eleven percent (202) of children are Muslims while point four percent of children are Burghers.

Prevalence of Online violence against children.

Awareness Online Violence among Children.

Sixty eight percent (1,299) of children have heard of online violence while thirty two percent (612) have not heard of online violence. Nearly twenty eight percent (265) of boys and nearly thirty seven (347) percent of girls had not heard of online violence against children.

Table 4.9 Awareness of online violence by gender

Awareness of online violence	Gender		Total
	Boys	Girls	
Yes	700	599	1,299
	72.5%	63.3%	68.0%
No	265	347	612
	27.5%	36.7%	32.0%
Total	965	946	1,911
	100.0%	100.0%	100.0%

Source: Survey Data 2020

Though the number of children who are aware of online violence is comparatively higher, one third of children being unaware of online violence is noteworthy. In addition, it is also important to question the level of awareness of the children who have said that they are aware of online violence. The awareness of each child is subjective and their level of awareness may be limited to one or few types of online violence. Moreover, the children may not be aware about legal support available to them and ways of accessing support systems. Therefore, it is important to revisit the awareness programmes conducted by the government and the non-governmental organizations, and try and provide a holistic awareness to children.

The children identified the types of online violence they have heard of. These are listed in the table below:

Only just under thirty percent (565) of children identified sending indecent text messages as a type of online violence in comparison to other forms of online/cyber violence. This is a noteworthy factor as it could indicate that the prevalence and frequency of sending indecent text messages among children have amounted to a normalization by which children do not necessarily consider it to be a serious form of online violence. This was further surfaced during the focus group discussions conducted among children at district levels. In contrast, nearly eighty seven percent (1,566) of children identified sharing indecent pictures/cliparts/videos/texts/scripts/audios/clips/emails and nearly eighty two percent of children (1,566) identified online sexual harassment of a child as online violence. Furthermore, eighty one percent of children (1,555) stated cyber extortion and seventy four percent (1,424) identified continued requests sent by the same person as a type of online violence.

The key informants had mixed opinions about the awareness of children on online violence. Most of the key informants stated that they believe that children lack a complete and comprehensive understanding of all types of online violence.

For instance, the representatives from Save the Children were of the opinion that children's definition of online violence can be highly subjective. They used sharing nude pictures as an example and explained that normalization of sharing nudes and videos with sexuality has made it difficult for the children to identify it as online violence. ***“For example, if a child is in a relationship, the boyfriend or girlfriend requests for a nude photograph as an expression to show that one is committed to the relationship. In addition, saying that it is happening among peers. Then they would probably not think twice before sharing such photographs.”*** (KI Interview, 2020).

Table 4.10 Types of online violence (Multiple Responses)

Type of online violence	Gender		Total
	Boys	Girls	
1. Sending indecent text messages	283	282	565
	29.3%	29.8%	29.6%
2. Sharing indecent pictures/cliparts/videos/texts/scripts/audio clips/emails	809	822	1,631
	86.9%	85.3%	86.9%
3. Online sexual harassment of a child	806	760	1,566
	83.5%	80.3%	81.9%
4. Cyber Extortion	780	775	1,555
	80.8%	81.9%	81.4%
5. Online sexual harassment of a child	727	697	1,424
	75.3%	73.7%	74.5%

Source: Survey Data 2020

The representative from LEADS also shared this opinion. ***“It is difficult to say that they don’t know about it and also to say that they are hundred percent aware of what it is. It is difficult for them to have a clear-cut understanding about whether a certain act is an offence.”*** (LEADS, 2020)

The findings suggest that children require further awareness of online violence against children and to how to identify them.

Expert definitions of online violence against children in Sri Lanka

The study also explored opinions of key stakeholders involved in child protection and welfare. The key informants (KI) gave various definitions of “online violence” and each definition looked at the phenomenon using different approaches such as the rights approach, the power approach and the cyber specific approach.

A child protection expert defined online violence as a violation of children’s rights and “an act of misusing power against any party using the internet, [thus] violating their rights” (KI Interview, 2020). This definition suggests the existence of power dynamics between two or more internet users and the definition proposes that the power dynamic is equal between the two users as long as both users do not compromise information or data about the other party. The equilibrium of power shifts when a party obtains sensitive and possibly harmful data about the other party. The internet user with greater power may or may not then go on to exploit sensitive information to violate the rights of the child.

A cyber security expert described online violence in the following manner; “if a child is subjected to any act leading to mental or physical abuse as a result of internet online-based activity, it can be called online violence” (KI Interview, 2020). The respondent went on to say that, “the online abuse can later lead to offline violence” (KI Interview, 2020).

The KI interviews revealed the lack of a universal definition of online violence against children. As emphasized by a representative of a global policing agency “the lack of common definitions and terminologies is a key challenge as it might cause confusion or lack of understanding, and even hinder the effective prevention and elimination of online violence” (KI Interview, 2020).

Experiencing Online Violence

Twenty eight percent of children have experienced some kind of online violence. In other words, three out of every ten children interviewed in the study have experienced some sort of online violence. This finding is extremely significant as it reveals the magnitude of the issue, showing that immediate measures have to be taken to curb and mitigate online violence before it grows further. If not addressed immediately, online violence can have long term impacts on the lives of children in Sri Lanka.

Table 4. 11 Experiencing online violence by Gender (Multiple responses)

Type of online violence	Gender		Total
	Boys	Girls	
1. Yes, I have experienced online violence	264 27.35%	272 28.75%	536 28.05%
2. No, I have not experienced online violence	701 72.65%	674 71.25%	1,375 71.95%
Total	965 100.0%	946 100.0%	1,911 100.0%

Source: Survey Data 2020

The above finding also suggests that slightly more girls (29%) have experienced online violence compared to boys (27%).

Types of online violence experienced by children

The children identified different types of online violence that they have experience which are listed in table 4.6 below.

Table 4. 12 Types of online violence experienced by Gender (Multiple responses)

Type of online violence	Gender		Total
	Boys	Girls	
3. Receiving indecent text messages	251 27.3%	231 28.8%	536 28.0%
4. Receiving links and advertisements to indecent pictures/cliparts/videos/texts/scripts/audioclips/emails	258 26.7%	244 25.8%	502 26.3%
5. Receiving indecent pictures/cliparts/videos/texts/scripts/audioclips/emails	233 24.1%	232 24.6%	465 24.3%
6. Sexual harassment of a child	176 18.5%	219 23.0%	395 20.7%
7. Cyber Extortion	79 18.8%	217 22.7%	396 20.7%
8. Making sexual comments/indecent jokes about your body, appearance, a family member	171 17.7%	204 21.6%	375 19.6%
9. Sharing an indecent image of you	171 17.7%	204 21.6%	375 19.6%
10. Sending an indecent image that you did not request	190 19.6%	211 22.4%	401 21.0%
11. You clicking on a link in a message sent to you that showed indecent images of other people	211 21.8%	226 23.9%	437 22.9%
12. Identity theft (Someone hacking your profile/Someone creating a fake profile using your details and images)	163 16.9%	194 20.6%	357 18.7%

Source: Survey Data 2020

Receiving an indecent message is the most common type of online violence (twenty eight percent- 536). Nearly twenty eight percent of boys (264) and nearly twenty nine percent (272) of girls had experienced this type of violence. Receiving links and advertisements has a percentage of over twenty six percent of (502). Irrespective of gender children of both genders have suffered due to online violence; however girls have suffered slightly more compared to boys. The findings revealed the prevalence of various types of online violence against children in Sri Lanka. These include

- (i) Child Sexual Abuse Material (CSAM)
- (ii) Online extortion of children
- (iii) Identity theft
- (iv) Online sexual harassment of a child

Child Sexual Abuse Material

The key informants identified Child Sexual Abuse Material (CSAM) to be one of the most prevalent type of online violence in Sri Lanka. CSAM is material depicting acts of sexual abuse and/or focusing on the genitalia of the child (ECPAT, 2016). These materials can depict children in any age group, any gender and includes all types of sexual abuse. The nature of CSAM can be commercial or non-commercial.

Revenge Porn

Revenge porn is also referred to as online rape, nonconsensual pornography, involuntary porn, or image based sexual abuse. It refers to the publication of

sexually explicit images or videos on an online forum (Citron and Franks 2014; Henry and Powell 2016; McGlyn et al. 2017b; Walker and Sleath 2017). Usually ex-partners who use sexually explicit text messages, photographs or videos can commit revenge porn. Moreover, such materials are accessible remotely by means of hacking. According to an official from World Vision, he had come across cases of this nature.

In an interview with officials from the National Child Protection Authority, it was emphasized that self-produced sexual material has become a serious concern. In some cases girls have produced sexual material such as pictures and videos and had shared them with their partners (often as per the request of the boyfriend/s). Once the relationship ends, the boyfriend

Sharing of self-produced CSAM

“Recently we came across a case of a girl who had made a compromising video of herself. She had recorded the video with her boyfriend’s phone and had given it to him without telling him about the video. So by mistake the boyfriend had attached the video to another set of videos and shared it among friends using the Shareit app. Once the girl found out about this she had informed her parents who sought the support of the police to put an end to the sharing of the video”

—— KI Interviews, 2020

distributes these sexual material using online platforms such as end-to-end encrypted social media sites such as WhatsApp. A key informant went on to say that *“one thing I have seen is sharing of sexual images and videos of a girl who is part of my youth group. A girl has sent nude pictures of her to a boy she had liked and he had shared these pictures with his friends. Now she is afraid of talking to boys”* (KI Interview, 2020).

According to an official from the Grassrooted Trust, often boyfriends make their girlfriends share their nude pictures and videos by convincing them that it is a part of their relationship. If a girl refuses to share such pictures, they would pressurize the girls saying *“you are the only girl friend who has not sent a picture to me, all my other friends get such pictures”* (KI Interviews, 2020).

Self-generated sexual content

The existence of revenge porn has also given rise to sharing of self-generated sexual content and using them as an exchange commodity to access CSAM generated by others. In an interview with an official from Grassrooted Trust, he revealed an alarming case that he had come across in 2015. His organization was informed about a group of organized perpetrators who collect CSAM material

by contacting boyfriends and ex-boyfriends of girls. They had amassed a large database of CSAM material and were offering others access to the database as long as they shared CSAM that they did not have in return. According to the official *“basically, the database screenshots were sent to boys saying this is what we have, we know you are going out with X. If you send a picture or video of X we will give you access to this database. Then in 2018 or 2017, we were informed of a price list which was going around in schools. The price list ranged from 500 rupees for a picture revealing the upper body-breast up to 2,500 rupees for a close-up picture of the vagina”* (KI Interviews, 2020). The findings suggest that CSAM material has become a

commodity in some circles, and a supply and demand has sprung up for such material, creating a vicious cycle of CSAM.

Extortion of Children

Extortion of children was another type of online violence which was mentioned by the key informants. The cases of extortion reported to the research team have a close connection to CSAM. The findings reveal that CSAM was used by boyfriends/ex-boyfriends and collectors of CSAM to extort the girls to produce and share more CSAM material. According to a former chairperson of the National Child Protection Authority, the same perpetrators who had approached the boyfriends of girls to collect CSAM material later changed their strategy and had approached the girls and extorted them to produce more CSAM by *“getting girls to send photos, more and more photos can be collected by extortion saying that we will publish other photos or send them to their parents”* (KI Interview, 2020).

In some cases, the girls were extorted and demands were made to give ransom in order to refrain from sharing nude pictures. In another case, a girl was threatened with a nude picture of her by her ex-boyfriend and the girl had resorted to pawn her mother’s jewelry to pay the ransom. The representative from the Grassrooted Trust also revealed that they had received cases where girls were forced to engage in sexual

Online Extortion of Children

“In another example, at a house the Mother’s jewelry Cabinet was broken into and the Jewelry was taken. The parents suspected the domestic worker and took her to the police station saying that she is the only one who could have perpetrated the crime. Then the daughter came out saying no I took the gold and pawned it for 70,000 rupees to give it to my boyfriend. He has a picture of me and is blackmailing me”

—— KI Interviews, 2020

intercourse with their boyfriend and ex-boyfriends. This exemplifies a correlation between online and offline sexual abuse/harassment.

The key informants also identified threatening and bullying as other types of online violence evident in Sri Lanka. The NCPA officers referred to a recent case where a group of children threatened each other using the Facebook social media platform. According to officers, a set of adults had forced the children to make these threats online: ***“In the recent situation about children acting out threatening other children, we got to know that individuals older than the children had forced them to make videos. We are now trying to investigate this further and apprehend them. According to the law of Sri Lanka it is a crime to use a child in obscene videos or imagery. Parents have a responsibility to check on what their children are doing on the internet (NCPA, 2020).***

Online Platforms and Experiencing Online Violence

The children who had experienced online violence mentioned the websites and applications they used when they experienced such instances. The applications and websites are listed in the table 4.13.

Table 4. 13 Online platforms where online violence was experienced by gender (multiple response)

Online Platform	Gender		Total
	Boys	Girls	
Facebook	131	73	204
	74.0%	57.9%	10.67%
Instagram	72	65	137
	40.7%	51.6%	7.16%
Twitter	45	51	96
	25.4%	40.5%	5.02%
Imo	53	42	95
	29.9%	33.3%	4.97%
Viber	34	24	58
	19.2%	19.0%	3.03%
WhatsApp	54	29	83
	30.5%	23.0%	4.34%
Pinterest	19	9	28
	10.7%	7.1%	1.46%
Messenger	42	13	55
	23.7%	10.3%	2.87%
Wechat	12	2	14
	6.8%	1.6%	0.73%
Tik Tok	22	8	30
	12.4%	6.3%	1.56%
Google	31	8	39
	17.5%	6.3%	2.04%
Yahoo	5	2	7
	2.8%	1.6%	0.36%
Gmail	7	1	8
	4.0%	0.8%	0.41%
y mail	2	0	2
	1.1%	0.0%	0.10
PUBG	6	2	8
	3.4%	1.6%	0.41
Online games	1	8	9
	0.6%	6.3%	0.47
YouTube	13	10	23
	7.3%	7.9%	1.20
Chrome	10	1	11
	5.6%	0.8%	0.57
Mozilla	0	1	1
	0.0%	0.8%	0.05%
Did not respond	87	146	233
	9.01%	13.31%	12.9

Source: Survey Data 2020

In terms of children who reported that they experienced some form of online violence, most of them had experienced such incidents of online violence while using Facebook (Boys—Nearly 74%/Girls—nearly 58%). In addition, children have suffered while using Instagram (Boys – nearly 41%/Girls – Nearly 52%) and while using the Twitter application (Boys – 25%/Girls- Nearly 41%). This reveals that children using all online applications are exposed to online violence.

Reaction of Children to Experiences of Online Violence

Experiencing online violence could trigger many reactions in a child. Some children might consider online violence as a mere nuisance while some children may consider violence to be a serious threat to them and their immediate circle. The children identified multiple reactions they had when they experienced online violence. Their reactions are listed in the table below.

Table 4.14 Reaction to online violence by gender (Multiple Response)

Response	Gender		Total
	Boys	Girls	
I ignored the problem or hoped that the problem would go away by itself	103	80	183
	39.01%	29.41%	34.14%
I closed the window or app	55	20	75
	20.83%	7.35%	13.99%
I felt a bit guilty about what went wrong	24	14	38
	9.09%	5.14%	7.08%
I tried to get the other person to leave me alone	12	7	19
	4.54%	2.57%	3.54%
I tried to get back at the other person	5	2	7
	1.89%	0.73%	1.30%
I stopped using the internet/app for a while	13	19	32
	4.92%	6.98%	5.97%
I deleted messages from the other person	21	6	27
	7.95%	2.20%	5.03%
I changed my privacy/contact settings	16	5	21
	6.06%	1.88%	3.93%
I reported the problem online	4	4	8
	1.51%	1.47%	1.53%
I followed the instructions of the person	6	8	14
	2.27%	2.94%	2.61%
I don't Like to share my reaction	5	107	112
	1.93%	39.33	20.89
Total	264	272	536
	100.00%	100.00%	100.00%

Source: Survey Data 2020

Over thirty four percent of children (183) had ignored the issue and hoped that it would go away by itself while nearly fourteen percent (75) of children had closed the window or app. Over seven percent of children (38) stated that they felt guilty about what went wrong and nearly six percent of children stated (32) that they stopped using the application for a while. Nearly three percent (14) stated that they followed the instructions of the person. The reactions of the children reveal that majority of the victimized children had felt the experience to be a nuisance but did not resort to take legal measures or inform someone else about the violence. They have resorted to take ad hoc and relatively ineffective action such as leaving the website or closing the app and refraining from logging into the online platform for a while.

Help Seeking Behaviour

Nearly forty four percent of children had informed another individual about online violence. Twenty percent of children had not informed anyone about the incident. Majority of children (over twenty percent) had informed either peer or a friend older than him or her about the instance of online violence. Nearly twelve percent of children (62) had informed a parent about the incident. This reveals that children are more likely to share an experience of online violence with a peer than an adult. The children who participated in the district level focus group discussions stated that the generational gap between themselves and adults, and being afraid of being further victimized by adults deters them from revealing experiences of online violence to adults.

Table 4.15 Informing someone about online violence by Gender

Person	Gender		Total
	Boys	Girls	
My mother, or father/Guardians	30 11.36%	32 11.76%	62 11.66%
Siblings	13 4.92%	13 4.77%	26 4.95%
Cousins	6 2.28 %	1 0.36%	7 1.40%
A friend around my age	81 30.69%	36 13.23%	117 21.82%
A friend who's older than my age	8 3.03%	6 2.20%	14 2.61%
A teacher	3 1.13%	2 0.75%	5 0.95%
Another adult I trust	2 0.76%	1 0.39%	3 0.55%
I didn't talk to anyone	57 21.59%	51 18.75%	108 20.14%
Prefer not to say	64 24.24 %	130 47.79%	194 36.19%
	264 100.0%	272 100.0%	536 100.0%

Source: Survey Data 2020

Children also mentioned about when they confided in someone about the online violence.

Table 4.16 When they informed – by gender

Response	Gender		Total
	Boys	Girls	
On the very day it took place	51 19.31%	51 18.81%	102 19.02%
The very next day	37 14.01%	20 7.41%	57 10.67%
Few days after	37 14.01%	16 5.88%	53 9.88%
A week after	21 7.95%	6 2.20%	27 5.03%
After a month	5 1.92%	6 2.20%	11 2.05%
Did not respond	113 42.80%	173 63.50%	286 53.35%
Total	264 100.0%	272 100.0%	536 100.0%

Source: Survey Data 2020

Out of the children who had experienced online violence majority (102) of the children who had suffered from online violence had informed someone the same day while 57 had informed someone the very next day. 53 had informed someone a few days after the incident while 27 children had informed someone after a week.

Table 4.17 Response of the individual the child confided in – by gender

Response	Gender		Total
	Boys	Girls	
Supported you in complaining to the authorities	22	19	41
	8.33%	6.98%	7.65%
Listened to you but did not take any action	54	28	82
	20.45%	10.32%	15.30%
Listened to you and advised you not to take any action	15	10	25
	5.68%	3.67%	4.67%
Listened briefly and blamed you	42	21	63
	15.93%	7.72%	11.75%
Did not listen to you or take any action	9	5	14
	3.40%	1.83%	2.61%
Do not like to respond	122	189	311
	46.21%	69.48%	58.02%
Total	264	272	536
	100.0%	100.0%	100.0%

Source: Survey Data 2020

Majority (82) of the children who had experienced online violence had not received any help from the person they confided in while only forty one had helped them to complain to authorities. 25 children had been advised by the person they confided in, to refrain from seeking help from authorities while 63 had been blamed by the person they confided in.

Reasons for Not Seeking Help

The children who had experienced online violence but had refrained from telling anyone stated reasons for not seeking help. These reasons are listed in the table below.

Table 4.18 Reasons for not seeking help – by gender

Response	Gender		Total
	Boys	Girls	
I was scared	23	38	61
	8.71%	13.97%	11.38%
I was threatened with my life	9	7	16
	3.40%	2.75%	2.98%
I was threatened with revealing personal information	18	7	25
	6.81%	2.57%	4.66%
I was offered gifts/money/ goods to keep it as a secret	6	8	14
	2.27%	2.94%	2.61%
I was offered gifts/money/goods to do this	2	2	4
	0.75%	0.73%	0.74%
I didn't want to lose that friendship /relationship	2	0	0.37
	0.75%	0.0%	0.1%
He/she offered me emotional support	1	0	1
	0.37%	0.0%	0.18%
He/she was there for me when no one else was there	4	4	8
	1.51%	1.47%	1.49%
I didn't care	4	3	7
	1.51%	1.10%	1.30%
Not applicable	195	203	398
	73.86%	74.63%	74.25%
Total	264	272	536
	100.0%	100.0%	100.0%

Source: Survey Data 2020

Fear

Of the majority (61) of the children who did not share their experience with anyone else stated that they were too scared to complain to an authority. 25 children stated they were threatened with revealing their personal information if they reported to authorities. Sixteen children stated they received death threats. Another 14 children stated that they were given gifts to keep the online violence as a secret. The focus group discussions with children revealed that children are afraid to seek help due to following reasons. One, due to the fear of being further victimized; for example one girl went on to say **“most of the time the parents, the adults and even the police blame the girl. They question why she shared a nude picture with her boyfriend, what other things she has done or whether she has sent other pictures or videos. Even the memory of such an issue is painful. No one would want to relive that again and again. Better to be silent”** (FGD, 2020).

Unaccommodating Parent-Child Relationships

In addition, it is evident that the relationship between children-parents/ children-teachers are a serious deterrent to help seeking behavior. The key informants also shared the opinion that often parents and teachers would further victimize the child, making him or her the culprit instead of supporting the child to seek help and to apprehend the perpetrators. According to the key informant from LEADS International, **“one reason could be the way parents/ teachers perceive and react to online violence. Often children – parent relationships are not modeled in a way that allow children to discuss these types of sensitive issues and children might be afraid that they might lose friends by disclosing these issues (KI Interview, 2020).**

Lengthy Legal Process and Re-victimization in the Process

Secondly, due to the fear of their future being affected by seeking legal support. One girl stated in a focus group discussion **“from what I have heard, when you complain to the police you have to visit the police station many times and then to the courts for years. If something like this happens to me all I would want to do is to forget that it ever happened and start life anew. But when legal action drags on forever it never allows you to forget about it. Then the people in the village also get to know about the issue and that creates another issue as people start to see you as less of a person” (FGD, 2020)**

The officials of the NCPA stated that children and parents are reluctant to seek help from legal authorities as the legal process takes a long time. They stated that children have to report to the court multiple times and it is cumbersome to both the child and the parent. The key informant interviews suggest that cases of online violence takes a significant time to conclude and by the time the court proceedings are over children have become adults and some are even leading married lives and have children of their own. Such long court proceedings could prolong the suffering of the child and the prospects of finding a life partner to lead a normal life.

The Lengthy Legal Process and Fear of Further Victimization in the Process

“Recently there was a case where the parents were planning to send the child to Australia for higher education. Therefore, the parents were reluctant to lodge a complaint thinking that this would create issues for the child’s education. Often we see that child abuse cases take a significant time to be resolved. So this discourages children and their parents from making complaints”

Difficulties in Accessing Legal Support

In another interview a representative from the Grassrooted Trust stated that children and parents have experienced difficulty in accessing legal support. He further said that most police officers lack awareness on where to complain and how to complain regarding cases of online violence. **“Majority of the children don’t go to the police because the children do not consider them to be a serious offence. Secondly where can they go?... (KI Interview, 2020).**

Difficulties in accessing law enforcement authorities

In one case in Monaragala, the parents had gone to the police and the police had asked them to go to the CID as they do not have jurisdiction to investigate these cases. When they went to the CID they had said that the case had taken place in Monaragala so to lodge a complaint in Monaragala. The family then got tired of this and they decided not to proceed with further legal action”

———— KI Interviews, 2020

Characteristics that make children vulnerable to online violence

The children identified characteristics that make them vulnerable to online violence. Majority (sixty three percent) identified the lack of supervision of parents as a key characteristic, while nearly twenty eight percent (532) identified lack of awareness of online violence as another key characteristic. In addition, nearly forty four percent of children stated sharing personal information publicly as a risky characteristic.

Table 4.19 Factors that make children vulnerable to online violence – by gender (Multiple Response Question)

Factor	Gender		Total
	Boys	Girls	
Lack of awareness about cyber violence	255	277	532
	26.4%	29.3%	27.8%
Lack of supervision by a parent	592	619	1,211
	61.3%	65.4%	63.4%
Sharing personal information publicly	377	461	838
	39.1%	48.7%	43.9%
Trusting people you meet online too much	418	467	885
	43.3%	49.4%	46.3%

Source: Survey Data 2020

Echoing some of the findings from the children and interviews carried out with the key informants, one can identify many characteristics that make children vulnerable to online violence. These characteristics include:

Gender of Children

The gender of children can play a role in making children vulnerable to online violence. However, the empirical data of this research indicated only a slight difference between the two genders in experiencing online violence. Majority of the key informants agreed that girls are more vulnerable to online violence than boys. The officials of the NCPA stated, **“girl-children are more susceptible to online sexual violence by locals”** (KI Interviews, 2020). A former chairperson of NCPA stated **“firstly, it is more difficult to extort or bully a boy because the repercussions for boys are not severe compared to a girl”** (KI Interview, 2020). The power dynamics attributed to the two genders make girls seem more vulnerable than boys in the online world similar to that of

the offline world. **“Masculinity is a deep rooted issue. When we talk about online violence, the solutions are not just about online violence. It is just how our society works. The same factors are making children vulnerable and making it very difficult for them to seek help.....I don’t think it’s different from offline abuse”** (KI Interview, 2020).

Over confidence about internet use

The representative from the Internet Watch Foundation stated that over confidence of children can be a characteristic. According to her some children believe that they can determine the age and gender of people they interact with. **“Sometimes children are over confident about their internet use; they tend to think so especially when they use a platform exclusively used by peers. We have identified that a broad education is needed for the children and that it is difficult to determine whom we are talking to online.”** (KI Interviews, 2019).

Lack of parental supervision

A representative of Sarvodaya-Fusion identified the lack of parental supervision to be a characteristic for increased vulnerability. The KI children stated that as a result children get into friendships and relationships with individuals who are much older than they are or who have malicious intents. **“When young children access internet without parental supervision they are vulnerable. Some children who do not know how to select friends online accept any request without checking the background”** (KI Interview, 2020). It is clear that the supervision of children’s online usage is compulsory as children lack awareness and intuition to identify attempts of online violence against them. Parents should be able to guide children who use online platforms, interactions made on social media and interactive platforms. However, it is evident from this research study that this is currently hardly achievable as many parents in Sri Lanka lack awareness not only about forms of online violence, but also about the technology itself.

Using internet for a long period

Other key informants identified that using the internet for long periods, especially playing online games can make them vulnerable to online violence. According to the representative from World Vision **“spending too much time on online games can be a major reason or a factor as children engage for a long period of time and often they bully and verbally harass each other. So that can be a characteristic”** (KI Interviews, 2020). This opinion suggests that the time children spend on the internet has to be safe. Nevertheless, it is important to stress that limiting the time spent online should be carried out without unnecessarily barring children from using internet.

Sharing pictures and personal data on internet

The representative from Sarvodaya-Fusion identified that uploading pictures and personal information such as whereabouts, age, schools and acquaintances can make children more vulnerable to online violence. **“Another characteristic is uploading pictures and personal data to the internet without thinking twice”** (KI Interview, 2020). Such behaviour allows perpetrators to identify possible targets, their online patterns, to develop convincing back stories and to groom children.

The Impact of Online Violence on Children

Period of Impact

The children were asked about the period they felt upset or hurt due to the online violence they experienced. The responses of the children are listed in the table below.

Table 4.19 Period of impact – by gender

Response	Gender		Total
	Boys	Girls	
1. I got over it straight away	99 37.5%	60 22.05%	159 29.66%
2. I felt upset for a few days	40 15.15%	34 12.5%	74 13.80%
3. I felt like that for a few weeks	15 5.68%	11 4.04%	26 4.85%
4. I felt like that for a few months or more	26 9.84%	7 2.57%	33 6.15%
5. I still feel the same	15 5.68%	12 4.41%	27 5.03%
6. Prefer not to say	69 26.13%	148 54.41%	217 40.48%
Total	264 100.0%	272 100.0%	536 100.0%

Source: Survey Data 2020

Majority of the children who had experienced online violence stated that they got over the incident straight away (159) while seventy four children stated that they were upset for a few days. Thirty children stated that they felt upset for a few months while twenty seven children stated they still feel upset about the online violence. It is possible to infer that the impacts of online violence are both short term and long-term.

These include,

(1) Social isolation

The child might try to isolate themselves from their family, friends and peers as he or she might start to feel worthless or afraid to associate with any of them. This mainly happens as a result of the fear of victimization of children at home or at the hands of peers. In addition, in some instances the perpetrators try and convince the children that they are responsible for what happened to them and in such a situation the child might be distraught and feel responsible for the abuse they experienced. Such isolation may lead to personality disorders or even mental health issues.

(2) Behavioural and mental health issues

According to the representative from Save the Children, as an after effect of online violence, some children experience changes in their behavioral patterns which are triggered by changes in their biochemistry, **“violence affects the chemistry of a child’s brain: when faced with violence, children often enter a survival mode. Once they do, hormones associated with a fight-or-flight response are triggered inside children’s brains. These hormones can fracture the development of neural connections in the brain, inhibiting physical growth and decreasing children’s ability to learn”** (KI Interview, 2020).

(3) Exposure to further exploitation and abuse

Children also become vulnerable to further abuse. In the case of CSAM, the children are re-victimized each time the material is distributed or downloaded. According to a key informant, children require a tailor made support system that suits their needs. **“Each time an indecent image of a child is viewed or shared the child is re-victimized. It is horrifying for a victim to think of the images being viewed and circulated online so it is important that they are reported and removed as quickly as possible.”** (KI Interview, 2020).

Majority of the children stated that reaction of parents and school, and the type of violence decide the longevity of impact. A former chairperson of NCPA stated, **“it depends on the reaction of the families and on the type of the abuse. If the parents and schools react like it is the end of the world, it becomes a long term problem”** (KI Interview, 2020).

Awareness of the key stakeholders

This section explores the awareness of and support extended by parents, educators and mass media outlets in tackling online violence against children as judged by the children themselves.

Parents' awareness of online violence against children

Table 4.20 Awareness of parents – by gender (according to children)

Response	Gender		Total
	Boys	Girls	
Yes	219	295	514
	22.7%	31.2%	26.9%
No	746	651	1,397
	77.3%	68.8%	73.1%
	965	946	1,911
	100.0%	100.0%	100.0%

Source: Survey Data 2020

The children stated that parents in general lack an understanding about how the internet works and how to seek support when a child has experienced online violence. A representative from Mobitel Sri Lanka stated that often parents are unaware about the internet use of children; **“we have seen that most parents are ignorant; especially when you go beyond Colombo the ignorance is very high. Often the packages we issue for elderly individuals such as UPAHARA usually ends up in the hands of the youngsters”** (Key Informant interview, 2020).

Another key informant stated that parents face a difficulty in understanding that mobile phones can function as a computer **“Some parents have told me that the computer is kept where they can see it. Then I ask whether they have a phone. They say yes, and very often it is a smart phone”** (KI Interview, 2020). These findings suggest that parents lack awareness on internet usage as well as the possible harms of unsupervised online use. This seems to also affect the awareness of parents on the legal provisions available to children to combat online violence against children.

The children also stated that parents do not have a good awareness about the legal mechanisms available to them if their children experience online violence.

Table 4.21 Parents Awareness on legal mechanisms – by gender

Response	Gender		Total
	Boys	Girls	
Yes	340	210	550
	35.3%	22.2%	28.8%
No	607	713	1,320
	63.0%	75.4%	69.1%
Do not have an opinion	17	24	41
	1.76%	2.5%	2.14%
	965	946	1,911
	100.0%	100.0%	100.0%

Source: Survey Data 2020

Majority (Sixty nine percent) of children stated that parents do not have a good understanding on legal mechanisms available against online violence. Only nearly twenty nine percent of children believed that their parents had a good understanding. This lack of awareness can be a serious issue as it may deter parents from seeking legal support and worse, it can motivate them to discourage children from seeking legal support.

Table 4.22 Have parents discussed online violence with you? – by gender

Response	Gender		Total
	Boys	Girls	
Yes	580	652	1232
	60.2%	68.9%	64.5%
No	385	294	679
	39.7%	32.1%	35.5%
	963	946	1,911
	100.0%	100.0%	100.0%

Source: Survey Data 2020

Nearly sixty five percent of children's parents had talked with them about online violence, while nearly thirty six percent of respondent's parents had not spoken to them about online violence.

The children also revealed what their parents discussed with them. Their responses are listed in the table below.

Table 4.23 What parents discussed – by gender

Response	Gender		Total
	Boys	Girls	
Not to interact online with people we don't know	221 22.9%	249 26.3%	470 24.6%
Not to go to adult websites	398 41.2%	317 33.5%	715 37.4%
How to use internet for good things	37 3.8%	74 7.8%	111 5.8%
Not to initiate online romantic relationships	28 2.9%	40 4.2%	68 3.2%
Did not respond	281 29.1%	266 28.1%	547 28.6%
	965 100.0%	946 100.0%	1,911 100.0%

Source: Survey Data 2020

Over thirty seven percent (715) of children had received advice from their parents to refrain from using adult websites while nearly twenty five percent (470) of children have been instructed not to interact online with people they do not know in real life. Only just below six percent of children's parents had advised them to use the internet for good things/ positive objectives; and just over three percent of parents had warned children against engaging in romantic relationships online.

The findings suggest that majority of the parents have failed to discuss how the internet can be a useful tool and how they should obtain all the support that the internet can offer their children; and also be. ***In reality parents have tried to deter children from using internet instead of teaching them how to use the internet to obtain new knowledge and thrive for innovation, making them aware about the danger that internet can pose to them and also to inform them if a violence occurs to them.*** It is also interesting to note how none of the parents have instructed their children not

to use internet to harm a fellow internet user. It is important to cultivate ethical and fair use of internet amongst children and the instructions and supervision of parents can be instrumental in reducing the occurrence of online violence.

Educators' awareness of online violence against children

Table 4.24 Are educators aware about online violence? – by gender (according to children)

Response	Gender		Total
	Boys	Girls	
Yes	903 93.6%	908 96.0%	1,811 94.8%
No	62 6.4%	38 4.0%	100 5.2%
	965 100.0%	946 100.0%	1,911 100.0%

Source: Survey Data 2020

Nearly ninety five percent of children believe that educators have an awareness about online violence. Only five percent of children stated that educators do not have a good understanding of online violence. However, it is questionable whether the educators have a comprehensive understanding of online violence. Awareness of online violence should also infer awareness of legal measures, safeguarding confidentiality and providing support to the affected children. However, the next set of findings suggests that children are not very confident about seeking the support of an educator.

Table 4.25 Would you inform an Educator of an incident? – by gender

Response	Gender		Total
	Boys	Girls	
Yes	62	38	100
	6.4%	4.0%	5.1%
No	903	908	1811
	93.6%	96.0%	94.8%
	965	946	1911
	100.0%	100.0%	100.0%

Source: Survey Data 2020

When asked whether they would report a case of online violence to an educator majority (nearly 95%) of children stated that they would not. Only five percent of children said that they will inform an educator. The children further mentioned in the focus group discussions that they would also consider the trustworthiness of the educator and his personal qualities when trusting him or her with a serious matter such as online violence.

The children gave their reasons as to why they would not confide in an educator. The reasons they stated are listed in the table below.

Table 4.2 Why would you not inform an educator? – by gender

Response	Gender		Total
	Boys	Girls	
Because if they are informed they will create issues at school	90	99	189
	9.3%	10.5%	9.9%
Because it should only be discussed with parents	4	11	15
	0.4%	1.2%	0.8%
Because we are afraid of them	64	100	164
	6.6%	10.6%	8.6%
They do not consider online violence as a serious concern	6	3	9
	0.6%	0.3%	0.5%
Because teachers do not safeguard privacy or confidentiality	182	187	369
	18.9%	19.8%	19.3%
Because they will tell parents and the police	17	16	33
	1.8%	1.7%	1.7%
They do not listen to us	18	20	38
	1.9%	2.1%	2.0%
They blame the child most of the time	584	510	1,094
	60.5%	53.9%	57.2%
Total	965	946	1,911
	100.0%	100.0%	100.0%

Source: Survey Data 2020

Over fifty seven percent (1094) of children stated that educators often blame and victimize the child for online violence and over nineteen percent (369) stated they would not tell an educator as they do not protect confidentiality and privacy of children. Nearly ten percent (189) of children stated that educators would create issues at school, while nearly nine percent (164) said that they are afraid of their educators/teachers. Despite the improvement in awareness of online violence, the children stated that educators lack the ability and training to manage cases of online violence. A representative from LEADS stated that **“awareness has improved over the past few years. They are now more aware of what it is and what its impacts are. However, they do not have adequate experience in managing online violence cases. Those who train educators need to make them aware that in the penal code of Sri Lanka**

there are laws to tackle online violence. Then we need to improve how online violence against children are handled” (KI Interview, 2020).

Awareness of Internet Service Providers (ISP)

Awareness of Internet Service Providers by gender (according to children)

Table 4.27 Do internet service providers understand online violence? – by Gender

Response	Gender		Total
	Boys	Girls	
Yes	240	311	551
	25.0%	32.9%	28.9%
No	725	635	1,360
	75.1%	67.1%	71.2%
Total	965	946	1,911
	100.0%	100.0%	100.0%

Source: Survey Data 2020

Over seventy one percent (1,360) of children stated that mobile service providers do not have a good understanding of online violence.

Table 4.28 Have internet service providers taken enough measures to tackle online violence? – by gender

Response	Gender		Total
	Boys	Girls	
Yes	429	450	879
	44.5%	47.6%	46.0%
No	536	496	1,032
	55.5%	52.4%	54.0%
Total	965	946	1,911
	100.0%	100.0%	100.0%

Source: Survey Data 2020

Fifty four percent of children (1,032) stated that mobile service providers have not taken enough measures to safeguard children against online violence. The findings suggest that children believe that the Internet Service Providers (ISP) have a responsibility to the children. Specially, in terms of online violence children believed that ISPs should bring in new

technologies to block harmful material and provide them with a safer internet surfing experience. The key informant interviews also suggest that the ISPs are reluctant to spend resources and man power to help combat online violence against children and they are rather focused on improving their profits.

In addition, the key informants were highly critical of the internet service providers in Sri Lanka. The criticism is based on two grounds; one is that the ISPs have failed to take responsibility for the internet service they provide, and secondly the ISPs' lack of support to law enforcement. A former chairperson of NCPA stated, **“I think that internet service providers have to take on a lot of responsibilities. If someone uses my name to make a Facebook account, and if I want to prosecute, I should know who the person is. Finding that person should be done through ISPs. They don't have systems to make it easy. Therefore, ISPs need to take on the responsibility of helping law enforcement”** (KI Interview, 2020).

The representative from Grassrooted Trust further added to the same criticism and stated **“for an example when we need to identify a perpetrator we need to get a court order to get the information. When we get the court order the child is subjected to further abuse. They have a fast track system via the Sri Lanka Police. However, it is rarely used. The Police, NCPA, Children and Women's Bureau have to develop a system to quickly get this information”** (KI Interview, 2020).

Role of Mass Media

The research team explored the opinion of children regarding awareness, reporting with confidentiality and the awareness building role of mass media.

Table 4.29 Is Sri Lankan Mass media aware of online violence? – by gender

Response	Gender		Total
	Boys	Girls	
Yes	169	134	303
	17.5%	14.2%	15.1%
	0.1%	0.1%	0.1%
No	796	812	1,608
	82.5%	85.8%	84.1%
Total	965	946	1,911
	100.0%	100.0%	100.0%

Source: Survey Data 2020

Over eighty four percent of children (1,608) stated that Sri Lankan mass media is aware of online violence. However, the children who took part in the focus group discussions stated that mass media seems to lack a holistic awareness of online violence due to the way in which they portray the victimized children and their families. This became clearer when the children were asked about the nature of reporting of online violence against children by mass media.

Table 4.30 Nature of reporting incidents of online violence by gender

Response	Gender		Total
	Boys	Girls	
Ethically report cases of online violence	195	240	435
	20.2%	25.4%	22.8%
Do not report cases of online violence ethically	665	589	1,254
	68.9%	62.3%	65.6%
Don't have an opinion	105	117	222
	10.9%	12.4%	11.6%
	965	946	1,911
	100.0%	100.0%	100.0%

Source: Survey Data 2020

Nearly sixty six percent of children (1,254) stated that mass media do not report cases of online violence ethically. According to the children there are number of factors pointing to irresponsible reporting of online violence.

Table 4.32 Reasons given by children on why the media doesn't appropriately handle cases of online violence – by gender

Response	Gender		Total
	Boys	Girls	
They try to make profit out of online violence cases against children	103 10.7%	82 8.7%	185 9.7%
They broadcast programmes that highlight and sexualize children	43 4.5%	40 4.2%	83 4.3%
By broadcasting instances of online violence without protecting the privacy of the children they expose the victimized children to bullying and further harm.	45 4.7%	35 3.7%	80 4.2%
They only report child sexual abuse and ignore forms of online violence	5 0.5%	7 0.7%	12 0.6%
They do not have media guidelines when reporting about online violence	5 0.5%	12 1.3%	17 0.9%
They sensationalize online violence incidents	80 8.3%	81 8.6%	161 8.4%
The media further victimizes the affected family and children	26 2.7%	24 2.5%	50 2.7%
Sometimes they broadcast inaccurate information about the family and the children	46 4.8%	56 5.9%	102 5.3%
They do not protect the identity of children	612 63.4%	609 64.4%	1,221 63.9%
	965	946	1,911
	100.0%	100.0%	100.0%

Nearly sixty four percent of children stated that mass media organizations do not protect the identity of children while reporting and nearly ten percent stated (185) that media organizations try to make profit by reporting online violence. Over four percent of children (83) stated that media organizations broadcast programmes that sexualize children and another four percent (80) stated that media reports sometimes can lead to Sexual harassment of a child and further harm to victimized children. Over five percent of children stated that sometimes media broadcasts inaccurate information about the child and family which leads to further victimization of the child.

Another inference that can be made from the finding is that the media has a tendency to portray the child and his or her family as both the victim and the perpetrator. Often the mass media reports indirectly suggest that if the child was more smarter and if the parents were

more close to children instances of online violence could have been averted and as they failed to avert it. Such reporting could actually deter parents and children from sharing their experiences of online violence with the society and also provide the perpetrators a sense that they can get away with committing more violence.

Similar to the opinions about ISPs, the key informants were critical of the behaviour of mass media. All the children criticized the media for sensationalizing child abuse and irresponsible reporting. The representative from the Grassrooted Trust stated **“they are good at sensationalizing online violence. Very few articles properly explore the issue”** (KI Interview, 2020). Another key informant stated **“I believe that Mass Media actually do not want to advocate but they want to advertise. They twist the story and harm the privacy of children”** (KI Interview, 2020).

Despite the criticism, all the children agreed that if properly used, media can be a great tool to spread awareness and train parents and educators about online violence against children. However the Key Informants had a negative opinion about Mass Media and their effectiveness against online violence. The representative from the Grass Rooted Trust stated, **“It’s difficult to use media as responsible awareness mechanisms on gender based violence and domestic violence. Of course, well-designed paid advertisements have a long reach and a good impact but other than that, it is difficult to imagine that they will do much”** (KI Interview, 2020). The representative from PEaCE also agreed to this notion and stated that **“the Mass Media can play a major role to train teachers and parents about online violence. Unfortunately, they are lagging behind”** (KI Interview, 2020).

Chapter 05

Online Violence, Law and Children of Sri Lanka

This chapter looks at one of the key areas pertaining to the response of online/cyber violence against children in Sri Lanka – LAW. One of the key objective of this study had been to assess the nature and effectiveness of response and support mechanisms currently available for children in responding incidents of online/cyber violence committed against them. Naturally, one would expect the children to resort to legal support when they experience these types of violence in the cyber space. However, as already presented in the previous chapter, there are factors that deter children and their parents from seeking legal support. This chapter presents a brief analysis of the existing legal framework to protect children from online violence in Sri Lanka, and its shortcomings.

Brief Analysis of the Existing Legal Framework

a. Constitution of the Democratic Socialist Republic of Sri Lanka

The Constitution of the Democratic Socialist Republic of Sri Lanka includes a chapter on Fundamental Rights (FR). Article 12 of the Constitution stipulates that all persons are equal before the law and are entitled to equal protection of the law. This protection would extend to children as well. Article 12 (4)¹ however goes a step further and allows for special

provisions by law, subordinate legislation or executive action for the advancement of children. This provision recognizes the need for affirmative action for children as a special category that needs protection.

Apart from fundamental rights the Directive Principles of State Policy and Fundamental Duties (DPSP) mentioned in Chapter VI of the Constitution stipulates that the State is to promote with special care the interest of children and youth so as to ensure their full development, physical, mental, moral, religious and social, and to protect them from exploitation and discrimination.² However, as per article 29, this is a non-justiciable right. This shortcoming has however been overcome in fundamental right cases, where DPSP set out in Article 27 (2)(h) has been used in conjunction with Articles 12 and 12 (4) to protect the rights of children.³

b. Children's Charter of Sri Lanka The Government of Sri Lanka adopted the standards of the Convention on the Rights of the Child ("CRC") into State Policy by way of the Children's Charter ("CC"). As the basic policy document on Children in Sri Lanka, the Charter recognizes several international instruments on children with a focus on human rights in general.⁴ The Preamble to the CRC recognizes that the concern, care, nurturing, growth and development of children have been an

integral part of the indigenous traditions of Sri Lanka and its socio-economic and welfare policies.⁵ It further declares that the Constitution shall promote the interest of children and youth to ensure their full development and protection from exploitation and discrimination.⁶ In addition to this the Charter recognizes the protection of privacy of children,⁷ protection from abuse and neglect,⁸ protection from sexual exploitation⁹ and a responsibility on the state to organize appropriate social programmes for the prevention of physical or mental violence, maltreatment and exploitation and for the treatment of victims in achieving these objectives.

c. Penal code of Sri Lanka

Criminal offences in Sri Lanka are specified in the Penal Code. In respect of child protection, the amendments made to the Penal Code by Acts Nos. 22 of 1995, 29 of 1998 and 16 of 2006 are of paramount importance. The penal code amendment of 1995 introduced new offenses related to children and redefined existing offences whilst also increasing the applicable punishments.¹⁰ Section 286A introduces the new offence of "obscene publication and exhibition relating to children" under 18 years of age, which criminalized obscene or indecent exhibitions, shows, films, or photographs involving children. Accordingly making/producing/having in possession/importing etc. obscene writings, drawings, prints,

¹ "Nothing in this Article shall prevent special provision being made by law, subordinate legislation or executive action for the advancement of women, children or disabled persons"

² Article 27 (13) – Directive Principles of State Policy and Fundamental Duties.

³ In *Chandani De Soysa v. Minister of Education* (SC/FR. 2016/77), where the Court held that children living or affected by HIV have the full right to education and cannot be discriminated against such a ground with reference to Article 12 and Article 27 (2) (h) of the Constitution.

⁴ The Geneva Declaration of the Rights of the Child of 1924, the Declaration of the Rights of the Child adopted by the United Nations on 20 November 1959, the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights in 1976 (in particular in Articles 23 and 24), the International Covenant on Economic, Social and Cultural Rights also in the year 1976 (in particular in Article 10) and the statutes and relevant instruments of Specialized Agencies and International Organizations concerned with the welfare of children.

⁵ Sri Lanka Charter on the Rights on the Child: <http://www.childwomenmin.gov.lk/institutes/dep-probation-and-child-care-services/child-rights/crc>

⁶ 'The Constitution of the Democratic Socialist Republic of Sri Lanka that the State shall promote with special care the interest of children and youth so as to ensure their full development, physical, mental, moral, religious and social, and to protect them from exploitation and discrimination'.

⁷ Article 16

⁸ Article 20

⁹ Section 34: "The State shall take measures to protect the child from all forms of sexual exploitation and sexual abuse, and in particular to prevent – (a) the inducement coercion of a child to engage in any unlawful sexual activity; (b) the exploitation use of children in prostitution or other unlawful sexual practices; (c) the exploitative use of children in pornographic performances and material."

¹⁰ The offenses introduced/redefined by the 1995 amendment include, obscene publication and exhibition relating to children, cruelty to children, grievous hurt, sexual harassment, procuration, sexual exploitation of children, trafficking, rape (including statutory rape), incest, acts of gross indecency between persons and grave sexual abuse

paintings, printed matter, pictures, posters, emblems, photographs, cinematograph films or any other obscene objects are made punishable offences by this Act.

The amendment made in 1998 to the Penal Code introduced further offences related to children and accordingly causing or procuring children to beg, hiring or employing children to act as procurers for sexual intercourse and to traffic in restricted areas were made punishable offences. The Code also imposes a duty on developers of photographs or films to report any indecent or obscene photograph or film of a child they discover through their work, resulting in a penalty of imprisonment for up to two years and a possible fine. In 2006, the Penal Code was further amended Section 286B to extend the reporting duty to persons providing “service by means of a computer,” such as cybercafés to prevent the commission of sexual abuse of a child.¹¹ Further, Section 286C of the Penal Code was also introduced in 2006 to criminalize the storing or distribution of child pornography by email and the internet.

d. Obscene Publications Ordinance

Publication of an obscene article electronically is a criminal offence under the amended section 2 of the Obscene Publications Ordinance. Furthermore, the police and other law enforcement authorities file charges under the Obscene Publications Ordinance

(as Amended by Act, No. 22 of 1995 and Act No. 29 of 1998), when children under 18 years are found with cell phones with pornographic material, or in instances when children are provided access to obscene video films in internet cafes etc. It is apparent that the practical implementation of the act can be used as a defense against acts of OVAC.

e. Computer Crimes Act No. 24 of 2007

Under the Computer Crimes Act, No.24 of 2007, the offences are categorized into two areas: (a) committing of criminal acts such as stealing and fraud; (b) introduction of viruses, worms, unauthorized access, hacking and character assassination. Section 3 states that ‘any person who intentionally does any act, in order to secure for himself or for any other person access to – (a) any computer; or (b) any information held in any computer, knowing or having reason to believe that he/she has no lawful authority to secure such access and with the intention of committing an offence under the Act or any other law’. Illegal interception of data and unauthorized disclosures of information enabling access to a service is also included in the Act as an offence.¹² Section 7 makes it an offence for people to obtain information from a computer or a storage medium of a computer without permission. It also criminalizes downloading, uploading, or making copies of such illegally acquired content.

Although the aforementioned provisions do not directly address OVAC, they could be of vital importance in bringing perpetrators of online crimes against children to justice.

f. Policy framework

In reviewing the current policy framework on OVAC, the National Child Protection Authority (NCPA) of Sri Lanka is the leading authority for the protection of Children from all forms of abuse in Sri Lanka. It is entrusted with the role of promoting children’s welfare and interests at the national level. The National Policy on Child Protection 2017-2027¹³ prepared by the NCPA provides the overall framework of goals, guiding principles and values, policy goals and main strategies that can be adopted to ensure that all children are protected from all forms of abuse, neglect and other forms of maltreatment and harm. The policy goals and guiding principles and values of the Policy identify the phrase “other forms of violence and harm and child protection”¹⁴ as an umbrella term which may include OVAC. However, lack of express reference to OVAC is a notable drawback of the Policy.

The Policy¹⁵ encompasses the principles of ‘Best Interest of the Child’ as the primary criteria of all decision making affecting the lives of children. The best interests of a child will include assessment of both short and long-term risks of harm to the safety, wellbeing and development of the child. The principle of best interest of the child can play a significant role in addressing

¹¹ “Take all such steps as are necessary to ensure that such computer facility is not used for the commission of an act constituting an offence relating to the sexual abuse of a child”.

¹² Section 10

¹³ National Policy on Child Protection 2017, National Child Protection Authority and Ministry of Children Development and Women’s Affairs, <http://www.childwomenmin.gov.lk/storage/app/media/Draft-National-Policy-on-Child-Protection-SINHALA.pdf>

¹⁴ Policy Goal 1: All State stakeholders adopt evidence-based policies and programmes that uphold the principles of child protection and address the multiple fundamental factors that put children at risk of abuse, exploitation, neglect, and other forms of violence and harm, and empower families and children with the capacity to protect themselves and fostering resilience to adverse experiences.

Policy Goal 3: All State stakeholders develop within their institutions the skills, knowledge and attitudes specific to the child protection component of their primary focus and within the shared national framework of child protection and its principles to ensure that the policies and programmes that are implemented fulfill the spirit of this national policy, protection and its principles to ensure that the policies and programmes that are implemented fulfill the spirit of this national policy.

Guiding Principles and Values: These principles and values are underpinned by Sri Lankan law, Sri Lanka’s commitments under international law, and by best practices in the field of child protection globally.

¹⁵ Op.Cit. National Policy on Child Protection 2017

OVAC. This principle is stated in article 3 of the CRC.¹⁶ Children's parents or guardians must take appropriate measures to achieve this.

Gaps in the Sri Lankan Legal Framework – Responding to OVAC

Shortcomings of the Constitution of Sri Lanka –

This research identifies that there should be an independent and separate constitutional protection for children apart from affirmative action that is provided in article 12(4). Some noteworthy examples can be deduced from the Constitutions of South Africa, Nepal and Kenya where rights of Children are guaranteed through the inclusion of broader provisions with overarching stipulations to cover issues similar to OVAC. These examples are laid out below.

Article 28(1)(d) and (f) of the South African Constitution recognizes the right of children to be protected from maltreatment, neglect abuse and degradation and protects them from the performance of services which are inappropriate for their age and place their well-being at risk.¹⁷

In Nepal, the Constitution stipulates that victims of crime have the right to be informed of the progress of their case as well as the right to social rehabilitation and justice with compensation according

to law.¹⁸ Moreover, article 39(2) mandates that every child has the right to “education, health care nurturing, appropriate upbringing, sports, recreation and overall personality development from family and the State.” Sub-article (5) of the same article prohibits child marriage, illegal trafficking, kidnapping, or being held hostage. Sub-articles (7) (8) and (9) lay out that children should not be subjected to physical, mental, or any other forms of torture, guarantees their right to child friendly justice and special protection for vulnerable children while action contrary to sub-articles (4), (5), (6) and (7) is stated to attract punishment and compensation.¹⁹

Article 53 of the Kenyan Constitution specifies that children must be protected from abuse, that they must be subjected to parental care of both spouses and that a child's best interest is of paramount importance.²⁰

The provisions of the Constitution of Sri Lanka fall far short of this kind of protection for children.

Shortcomings of the Children's Charter

While the Charter covers key areas in protecting the rights of the children, it does not specifically provide for the protection of children from online violence. Additionally, neither the CRC nor the Children's Charter is justiciable (i.e. enforceable in any court of law), as there is no corresponding Act of

Parliament that incorporates the Convention into national law.²¹ Despite the salutatory provisions included in the Children's Charter, as it is a form of soft law, it does not have the capacity to be implemented before courts of law similar to a statute. This area of protection is therefore in dire need of hard law.

Nevertheless, the commitments enshrined in the Children's Charter are significant as they provide evidence that the government of Sri Lanka has exhibited a clear mandate and mechanism in place to implement its international obligations. Therefore, the relevant stakeholders have a significant role to play to promote legislative reforms and to make recommendations in regard to OVAC. Yet, policy framework aside, the inability to implement the provisions of the charter as binding legal provisions creates a lacuna in the existing legal framework of Sri Lanka.

Shortcomings of the Penal Code

Although the Legal Gap Analysis²² conducted by Verité research states that existing provisions in the penal code adequately provide legal relief against the online sexual exploitation of children, they have identified several issues that undermine the existing legal framework. The report explains that the Penal Code does not criminalize simulated representations or realistic images of children and the present terminology

¹⁶ 'In all actions concerning children, whether undertaken by public or private social welfare institutions, courts of law, administrative authorities or legislative bodies, **the best interests of the child** shall be a primary consideration.'

¹⁷ 28. (1) Every child has the right – (d) to be protected from maltreatment, neglect, abuse or degradation; (f) not to be required or permitted to perform work or provide services that (i) are inappropriate for a person of that child's age; or (ii) place at risk the child's well-being, education, physical or mental health or spiritual, moral or social development;

¹⁸ Art. 21. Right of victim of crime – (1) The victim of crime shall have the right to be informed about the investigation and proceedings of the case regarding his/her victimization. (2) The victim of crime shall have the right to social rehabilitation and justice with compensation as provided for by law.

¹⁹ Art. 39. Right of children – (2) Every child shall have the right to education, health care nurturing, appropriate upbringing, sports, recreation and overall personality development from family and the State. (5) No child shall be subjected to child marriage, illegal trafficking, kidnapping, or being held hostage. (7) No child shall be subjected to physical, mental, or any other forms of torture at home, in school, or in any other places or situations. (8) Every child shall have the right to child friendly justice. (9) Children who are helpless, orphaned, physically impaired, victims of conflict and vulnerable, shall have the right to special protection and facilities from the State. • State support for children; • Protection of victim's rights. (10) Any act contrary to Clause (4), (5), (6) and (7) shall be punishable by law, and children who have suffered from such an act shall have the right to be compensated by the perpetrator as provided for in law.

²⁰ Art. 53. (d) to be protected from abuse, neglect, harmful cultural practices, all forms of violence, inhuman treatment and punishment, and hazardous or exploitative labour; (e) to parental care and protection, which includes equal responsibility of the mother and father to provide for the child, whether they are married to each other or not; (2) A child's best interests are of paramount importance in every matter concerning the child.

²¹ A Legal and Institutional Assessment of Sri Lanka's Justice System for Children by the United Nations Children's Fund (UNICEF) Sri Lanka, Conducted by the Verité Research (Pvt.) Ltd., August 2017 – <https://www.unicef.org/srilanka/reports/legal-and-institutional-assessment-justice-system-children>

²² Sri Lanka: Online Child Sexual Exploitation: Legal Gap Analysis conducted by Verité Research, November 2019.

in the Penal Code does not expressly preclude the use of child pornography. Further, even if the Penal Code prohibits distribution of obscene publications of a child, it fails to address intent to distribute child pornography via computer systems. This omission weakens the protection system on distribution of child pornography.²³

The Global Study on Sexual Exploitation of Children in Travel and Tourism²⁴ identified that in relation to sexual exploitation of children online and related material, the Penal Code of Sri Lanka prohibits, 'child pornography'²⁵ under section 286 A.²⁶ However, this section does not provide a definition of 'child pornography' that incorporates the elements of the OVAC.

Shortcomings of the Computer Crimes Act —

This Act is insufficient to deal with situations of OVAC as it deals only with computer crimes pertaining to hacking, etc. and makes no mention of cybercrimes. The inadequacy of the provisions of the Act to deal with OVAC highlights that Sri Lanka needs to introduce new laws pertaining to addressing OVAC and consolidate existing laws relating to computer crimes in order to introduce a single, all-encompassing law to address cyber bullying, grooming, child pornography and other types of online violence. Hence, it is recommended that amendment of the Act should be made to make its investigatory provisions applicable to content related to cybercrimes as well as OVAC.

Shortcomings of Policy —

During the Focused Group Discussions, children responded to the question on how the incidence of OVAC can be prevented and the participants had a few grievances and adjacent recommendations. They suggested the existing laws should be further improved, new laws be implemented effectively and that the children be made aware of the laws and how to seek protection under the said laws. The children also advocated for harsher punishments for perpetrators of OVAC.

In addition to assessing potential threats in each circumstance, it is important to also review available resources for intervention. A forum in which potent threats are now alive and well is the internet. With the rapid development in technology children nowadays are no strangers to the online world. The policy falls short of its duty as far as it does not address the best interest of children with regard to two components – primarily enhancement of the knowledge in technology; secondly, the level safety is guaranteed from OVAC in the process of innocent use of such technology.

The NCPA being the mandated institutional mechanism charged with protecting the rights of the child must endeavor to craft strong policies, guidelines and other appropriate tools in combating OVAC in Sri Lanka.

The above findings and analysis demonstrate that the issue of OVAC in Sri Lanka needs to be addressed effectively in numerous ways, particularly by filling the gaps identified in the domestic legal and policy framework. Weakness in the legal framework as well as law enforcement will result in more victimization of children to OVAC. Therefore, the research proposes to address the gaps identified with a proper plan and this can be found in the section on recommendations.

Law and the Voice of Sri Lankan Children —

Through this study the children of Sri Lanka have voiced up their concerns regarding the laws and law enforcement pertaining to cyber/online violence against them. These findings have been presented in the previous chapter in detail.

One of the main questions posed in the survey was the adequacy of laws in curbing OVAC. The results revealed that 64.8% found the laws to be inadequate, while a meagre 35.2% had a positive response on the adequacy of the law. In terms of gender, 68% male children found the law to be inadequate while 32% were satisfied. Out of the female children that responded to the survey, 61.5% found that it fell short stated that the law falls short of the requisite level of protection and 38.5% found the relevant laws to be sufficient.

Perhaps the most important question that was posed whether the children would take legal action against the perpetrators of online violence. **An alarming majority of children, irrespective of gender – over 92% responded that they would not seek legal support or complain to legal authorities.** As detailed in the earlier chapter, **fear of further victimization** has been a key deterrent to seek legal support. In following up on the previous question, the participants were asked as to whom they would complain to **26.4% revealed that they would complain to the Sri Lanka Police, 48.2% preferred to approach the SLCERT and 17% chose to report to the NCPA.** It is troubling to see that comparatively only a lower percentage of children would see the support of the NCPA – the main law enforcement body for child protection in Sri Lanka.

²³ Ibid.

²⁴ United Nations Children's Fund (UNICEF) (2016), "The State of the World's Children 2016: A Fair Chance for Every Child", 136, accessed on 7 February 2017, https://www.unicef.org/publications/files/UNICEF_SOWC_2016.pdf. and ECPAT International (2016), "Global Study on Sexual Exploitation of Children in Travel and Tourism, Regional Report South Asia", 38, <http://globalstudysect.org/>.

²⁵ Ibid. ECPAT prefers the term 'child sexual exploitation images', at P.39.

²⁶ The Section recognizes the "offence of obscene publication and exhibition relating to children".

Table 5.1 Taking legal action against perpetrators

Would you take legal action	Gender		Total
	Male	Female	
Yes	50	43	93
	5.2%	4.5%	4.9%
No	891	871	1,762
	92.3%	92.1%	92.2%
Do not like to response	24	32	56
	2.5%	3.4%	2.9%
	965	946	1,911
	100.0%	100.0%	100.0%

Survey Data 2020

In the event the participants would not be willing to complain, they were asked of the reasons as to why they would refrain from lodging a complaint against their perpetrator and the results shed light on the various considerations that children consider. Unfortunately, as much as 30.3% males and 31.3% females felt that complaining would create further issues. 1.9% males and 1.6% females reported that they do not understand how to complain and 1.2% male children and 2.8% female children revealed that they would refrain from complaining out of fear. Further, 33.6% males and 42.2% females felt that there was little harm that could be caused from online violence and that there was no need to complain while, 33.4% males and 22.5%

females provided that they would be able to handle the situation themselves by blocking or unfriending the person. 1% of males and 1.9% females reported that they do not like to complain.

These concerns by children were further affirmed by the key informant interviews and the focus group discussions. In response to the question of whether the laws of Sri Lanka were adequate to prevent OVAC, the experts voiced the opinion that they were not. While acknowledging that there are certain provisions in the Penal Code that may prove useful, the lack of enforcement and prosecutions of such crimes were seen to render them ineffective. The lack of resources, refusal of the victims to

come forward and lack of coordination amongst authorities have been identified to be the reasons behind this. Further. Amendments have been recommended for the Penal Code to include crimes relating to OVAC as a direct crime as well as the enactment of specific laws to address them. The experts took note of the laws on extortion, harassment, computer crimes and publications of obscene images. However, the lack of specific laws to prevent OVAC was strongly felt. Importance of the contribution, involvement and proper training of practitioners, magistrates and judges in enforcing the mechanisms in place was also brought to the attention of the researchers. The lack of child-friendly laws was seen to be a major shortcoming along with the lack of awareness of existing laws on the part of parents. The FGDs revealed that Children lacked a clear understanding about the laws. While they were aware of the existence of laws they were not aware of the intricacies or the actual laws that exist to protect them. This postulates the need to raise awareness among children regarding the legal support available to them; and furthermore it is imperative to build their faith in the legal support systems available to them, especially that in the NCPA.

Chapter 06

Global Technologies and Avenues Available for Sri Lanka: Tech-driven Approaches to Tackle Cyber/Online Violence Against Children

Alongside the legal mechanism, this study has also looked into the tech-driven approaches/ mechanisms available to tackle cyber/online violence against children in Sri Lanka. The NCPA in collaboration with Save the Children has already established a Cyber Crimes/ Surveillance Unit to tackle cyber/online violence against children in Sri Lanka as a part of the Project to End Online Violence supported by the GPEVAC. The research team led by its cyber-security consultant had investigated some of the leading technologies available globally to respond to online violence. Having explored the feasibility of those avenues, this chapter has presented some of the low-cost tech-driven approaches that Sri Lanka can adopt.

Global Tech-driven Avenues

Due to the vast heterogeneity of online platforms, there are many surfaces available in the internet for online child abuse. Social media, messaging apps, emails, online chat groups, online games and live-streaming sites are the main pinpoint online resources, which reinforce online abuse. Main tech companies around the world have already devoted themselves to clear up this problem. In dealing with this matter, there are some sophisticated solutions available in the global tech-world.

- **Hashing Technologies** – Hashing algorithms are one-way mathematical algorithms, which generate digital fingerprints for input data. The algorithm cannot be used to regenerate original data from hash value (irreversible) and there will not be similar hashed value for different input data (Hash algorithm transforms any size input data into fixed length out. Therefore, there is extremely low possibility to have the same output

for different input data. This limitation can be mitigated using a more secure hash function). Based on the strength, hashing technology can use to identify child abuse content such images, videos, files in the network. To accomplish that, network operators should maintain an up-to-date hash value database of abuse contents binary value and should monitor contents of the network constantly. Some major impediments exist with binary hashing technology. Hashing technologies cannot detect new content, which is not marked as abuse content in their database. Hence, newly generated content can evade this mechanism without any doubt. Another limitation is that hashing algorithms work as one to one function; due to this if there is one-bit change in the abuse content, the hash function generates different signatures and then content can flow through the network without detection. The third drawback is it requires huge computational power as it needs to generate the hash value of each data file and then compare with hashed values of abuse contents. This adds a huge burden to user experience. The main strong point with hashing technology is that hashed databases can be distributed with external parties as the original content cannot be recovered from the hash value ("Hash Values– Fingerprinting Child Sexual Abuse Material", 2020).

- **PhotoDNA** – PhotoDNA is an enhanced version of hashing technology developed by Microsoft collaboration with Dartmouth College and then it was donated to organizations like NCME, project VIC. Furthermore, this technology is currently used by platforms like Facebook, Google etc. As reported by NetClean ("PhotoDNA", 2020), "PhotoDNA can identify a specific image regardless of its binary data. This is made possible because PhotoDNA looks at the visual content of the image, instead of exact binary image data. By calculating the mathematical distance (the Euclidean distance) between two PhotoDNA hashes it is possible to verify that the two hash values represent two different versions of the same image". So even there is slight modification in the image like resize, change format, PhotoDNA can identify as variation of original image ("PhotoDNA", 2020).

- **Blocking Technologies** – Blocking technology is the most widely used methodology to restrict access to abuse content. Generally, this operates at network level by blocking network traffic generated to specific domain names. Network traffic must be transferred through one of the Internet Service Providers (ISP)'s gateway (if it is not local network traffic). Therefore ISP can decide which network traffic should not transfer through their gateways. There are different methods to accomplish this task, which are indicated in the table below:

DNS Blocking DNS servers use to translate domain names into IP addresses, as the IP address is required to transmit network traffic in the network, not the domain name. If there is a black listed domain list, DNS server can prevent the transfer traffic to those domains. Even though this is a very straightforward solution, there are few drawbacks. The most adapted method to evade DNS blocking is VPN service. Other than that, the user can use a different DNS server, which does not block the domain. The third drawback is if a small part of a website contains illegal material this technology will block the entire site. As an example, DNS server has to block an entire social media platform, which makes it a naive tool. On the other hand, DNS blocking is a more cost efficient solution.

Deep Packet Inspection

•Rather than block traffic at network (Host names) level, DPI inspect the content of the traffic at application level. Which makes DPI more difficult to get round. For that reason, now ISP can identify respectively who use the abuse content of the social media, instead blocking the entire social media platform as DNS blocking. As always, there are some hindrances with DPI too. The main drawback is that today most of the traffic is encrypted, so DPI cannot identify abuse content in the encrypted data. Furthermore, this method can slow down traffic since it makes a bottleneck.

URL Blocking

Here instead of blocking the entire domain name, URL blocking makes it possible to block only specific web pages. As with the previous two methods, URL blocking is also vulnerable to VPN, TOR traffic.

Proxy Blocking

Proxy blocking provides an answer for previous methods, which could not provide an answer for encrypted traffic. Here Proxy servers operate as an intermediary who can decrypt traffic generated between source and destination. To get full advantage, this technology should be implemented at the ISP level and which makes it more cumbersome duty for ISP. In addition, of course, this method raises more issues with data privacy. ("Blocking Technologies – NetClean.com", 2020)

- **Web Crawlers** – Web crawlers are automated software used to index the content of the web pages by search engines. In the process of general web crawling, crawlers gather information about the web page like Meta tags. Afterward crawlers store the pages in the index so the search engine's algorithm can sort them for their contained words to later fetch and rank for users. Although traditional crawlers detect text content, some advanced crawlers like "ARACHNID" are programmed to scan the images on the site and inform the system about identified child abuse content. Then it needs to be verified by a human analyst to ensure that image contain child abuse contents. Final step is to inform the hosting provider about the material and inform them to remove it. In addition, value of the Project Arachnid is the ability to crawl in Dark net.
- **Keyword Matching** – Keyword matching is one of the most commonly used methods in many domains such as search engines, monitoring tools etc. When it comes to child abuse content analysis, key word matching identifies suspicious text contents in

online platforms. However having a predefined keyword set is a prerequisite for Keyword matching. Rather than a simple direct keyword matching, there are some advanced techniques like Fuzzy matching and Textual Analysis.

- Fuzzy Matching: The main limitation of the simple keyword matching technique is that it needs to appear in target content exactly the same way as the Keyword List. If there is a simple variation, it cannot identify. As a solution to this fuzzy matching algorithm will match even if there are variations.
- Textual Analysis: This is an application of Artificial Intelligence, which has capability to analyze documents with its semantic meaning. ("Keyword Matching", 2020)

- **AI based Solution** – Major restriction with Hashed based Technology, Blocking Technology and Keyword matching technology is that those can only identify previously recognized abused content. If those meet new abuse content, they fail to identify those as abuse contents. AI has the capability to identify new and

previously unclassified child sexual abuse material. Another problem with traditional approaches is that it needs a human analyst to endorse the validity of the content. However, AI can avoid that bottleneck too. When all put together AI, can conduct analysis and provide decision recommendations at a scale, speed and depth of detail not possible for human analysts. AI model's quality directly depends on the quality of the data set (training data). This is one of the obstacles developers have to face. In addition to that, it requires a lot of expertise and resources to implement such a system. Below section outlines some common AI applications in preventing, detecting and prosecuting online sexual abuse of children. (Bracket Foundation, 2019)

- Image Classification: To identify image contain child abuse contain or not
- Facial, Object recognition: To identify know victims, offenders, places etc.
- Natural Language Generator: To engage with offenders in social media or online forums
- Sentiment Analysis: To detect subtle sign of abuse
- Speech Recognition: To identify victim or offender from the voice

Tech-driven Approaches Feasible for Sri Lanka

Key informant interviews revealed that the Cyber Crime/Surveillance Unit of the National Child Protection Authority needed further support to enhance its operations. This includes both staff training and technological interventions/tools. However, funding stands as a barrier in obtaining advanced technological tools for its mission against cyber/online violence against children. Yet, the study has unearthed the following tech-options as the most feasible.

When it comes to Sri Lanka, the most viable technical solution is blocking technology. Due to its low cost nature, each ISP can implement DNS Blocking technique in their name servers. With respect to other blocking technologies

like Proxy and DPI, URL blocking ("Blocking Technologies – NetClean.com", 2020) technology requires much less computation cost since ISP just has to inspect the destination of the traffic rather than inspecting content in there. Which makes it more cost efficient to implement for ISPs. Even though other blocking methods have more benefits, ISPs have to spent more resources to implement such a solution. Regularly updating the black listed URL list improves the efficiency of the method.

Parental Control mechanism over digital devices is another solution. However, most of the parents lag behind when it comes to the use of new technology. Often children, have greater understanding of technology. However if the parental control mechanism is implemented at a lower level such as at the network or hardware level it will be more effective. If the mobile service providers can design a framework to filter out inappropriate contents for customers under the age of 18 similar to the British Board of Film Classification (BBFC), it would be well suited. Apart from that, around 30% of internet users are mobile internet users in Sri Lanka. Substantial users among them are teenagers. Having such a filtering framework for mobile networks is more applicable in the context of Sri Lanka.

Robust age verification system is another solution. Nowadays most of the local chat groups or web sites request to confirm age restriction by merely pressing a button. If there is a legitimate age verification mechanism to restrict access to digital content from those that are not appropriately aged, most of the online offense can be avoided. Deployment cost

of such a system is very low with respect to other technical methods. Furthermore, it has a high impact as DNS blocking and has more user experience than simply DNS blocking.

Since the most sophisticated web crawlers like ARACHNID already take charge of crawling method globally, there is no immediate requirement implement crawlers in local context. It is same as with hash technology, since organizations like IWF, Interpol keep record about globally available child abuse contents with help of advanced tools like PhotoDNA. A link can be developed between the local authorities and the international agencies. Such a link can be used get the support and the services of the international agencies to investigated CSAM cases. As an example when local authority get complain about child abuse content, they can use a web crawler to search them through online local community web sites to identify and remove them as immediate response ("Programs & Initiatives: Project Arachnid", 2020). The Keyword Matching Mechanism scans malicious content in the local chat groups since most of local companies do not interrogate child abuse contents in great depth. If there is a Keyword list (in Sinhala language) to implement such a mechanism, authorities can enforce local companies to adhere to the mechanism.

Dark Web is the biggest headquarters for child abuse activities. Study has found that over 80% of Dark-Web relate pedophile (Greenberg et al., 2020). As mentioned in the Technical solution section, even authorities could find child abuse content in specific location in dark web there

is no way to take them down since the anonymity of the publishers. Meanwhile, there is a very simple solution available to prevent children access into the dark web. It requires special software's like TOR browser or Browser Plugins to access the dark web. If those software's are rated as hazard apps (avoid access to children), children will not be able to download them into their devices.

Above section has discussed about how technical factor affect to online child abuse and their solutions. Most of the technical solutions have their own limitations. Still there is a very inexpensive but more beneficial factor, enormous impact to the problem, which is the human factor. In the online child abuse scenario, perpetrator has to lure victim into badness since there is no direct physical contact. If parents, tutors or administration can provide proper guidance to children about how to handle such situations, it will be more effective than technical solutions. For that, authorities can utilize expressive methods such as games, short films to reach younger generations regarding the trouble rather than simple presentations solutions.

Chapter 07

Recommendations

This study was conducted with an overall goal of understanding the seriousness of the online violence against children in Sri Lanka, thereby national strategies and policies to be informed and designed based on evidence provided by the study. The study especially focused on providing evidence to introduce a National Strategy to address Online Violence Against Children in Sri Lanka as part of the National Child Protection Policy implementation framework. The draft National strategy will be further informed and strengthened by the evidence and recommendations provided by this study. Therefore, our recommendations will be presented within key areas of the “Model National Response Mechanism” introduced by the WEPROTECT Global Alliance. A greater amount of these recommendations emanated from the participant children, hence it is their voice that one might find in these.

1. Policy and Governance

Sri Lanka has a progressive governance and policy landscape for children’s protection; however there is more to be done and those recommendations for ‘policy and governance’ cover the following key focus areas

- (a) National level government role and accountability
- (b) Situation analysis and monitoring of the threats and vulnerabilities to children and

- (c) Comprehensive and effective legal framework to investigate offenders and protection of victims.

1.1 The National Strategy developed to address online violence should be fully implemented along with the 5 year Action Plan to implement the National Child Protection Policy. The National strategy may be fully incorporated in to the Child Protection Policy Action Plan to create cohesive national strategy to address violence against children in Sri Lanka with an equal emphasis on online violence against children.

1.2 The Action Plan to implement the National Policy on Child Protection (NCPA, October 2019) and/or other child protection policies, strategies should adopt coherent definitions, terminologies and scoping to recognize the increasingly alarming threats and development of cyber/digital/online crimes committed against children.

1.3 The National Child Protection Authority (NCPA) should facilitate a uniform system to coordinate among the relevant agencies and authorities including the Attorney General’s Department, Telecommunication Regulatory Commission, SLCERT, Sri Lanka Police, all the relevant ministries, private sector actors, UN and

civil society actors to better improve and enforce laws, policies, and procedures to adequately prevent and respond to online violence against children. The actions that could be taken include CSAM content removal, online user administration, monitoring, international cooperation, victim support, rigorous punishment and penalties on perpetrators of violence. It is however pointed out that the monitoring of online activities should be done within the limits of legitimate privacy of individuals.

1.4 Sri Lanka is a State party to all the major international human rights instruments related to children. Therefore, Sri Lanka has the obligation to respect, protect and fulfill International Conventions and Agreements. In order to provide national enforcement for such Conventions and Agreements, national laws and policies should be formed and reformed in compatible with the UNCRC, optional protocol ii and other child rights instruments. Especially, the relevant organs of State should enact effective legislation, amend existing laws and interpret the existing laws to incorporate new developments.

NCPA

Incorporate a Special section on online violence against children to the National Policy on Child Protection.

Introduce technical and legal revision to Penal code sections:

286A, 286B, 288A, 288B, 308, 308A, 360B, 360C, 365, 365A and 365B, 368



SLCERT must function as the focal point for all types of online violence in Sri Lanka



Liability of parents, guardians, caregivers, principals and teachers as well as all adults who have knowledge about OVAC and omitted to protect children from it should be made criminally responsible for non-disclosure of know information.

1.5 The Budapest Convention should be adopted and recognized domestically without any reservations and must be looked to as basic guidance on matters related to OVAC. The Convention aims to pursue, as a matter of priority, a common criminal policy aimed at protecting societies from cybercrimes, building the capacity of countries to combat cybercrime, and functions as a mutual information sharing channel in order to facilitate better law enforcement. The legislature should take prompt action to meet these obligations and make necessary additions and amendments to the law. This should include measures to establish the offences listed in the Convention as criminal offences under the domestic law.

1.6 The Constitution of Sri Lanka – A child's best interests are of paramount importance in every matter concerning the child. However, currently, the 1978 Constitution does not include adequate Constitutional provisions to guarantee the best interests of the Child. It is recommended to introduce a new provision to the fundamental rights chapter to specifically provide for the rights, protection and care of children akin to the provisions included in the Constitutions of South Africa, Nepal and Kenya. Further, as the



Establish a ticketing system to track complaints lodged to NCAP. The ticketing system could be manually developed with the support of ICTA, University of Colombo School of Computing or an existing complaint management software such as Zendesk Support Suite or i-Sight Case Management.

current provisions on the Directive Principles on State policy are not directly enforceable in courts of law and remains non-justiciable, it is recommended that these duties of the State be amended in the forthcoming Constitutional Amendment to take on a justiciable form.

1.7 The Penal Code – The Penal Code does not adequately and explicitly provide for the protection, prevention and punishments for online related violence as articulated in the Budapest Convention. Therefore, technical and legal revision of Penal Code sections: 286A, 286B, 288A, 288B, 308, 308A, 360B, 360C, 365, 365A and 365B, 368 is important.

1.8 The definition of a child should be uniform across the existing legal framework in Sri Lanka. In the event it is not, the technicalities of age will cause a number of impediments to the law enforcement authorities. Therefore, the law should be amended to facilitate this.

1.9 “Cybercrimes” are defined generally as crimes committed through the internet using a computer. This includes a wide range of offences against computer data and systems (such as ‘hacking’), computer-related forgery and fraud (such as ‘phishing’), content offences (such as disseminating child pornography), and copyright offences (such as the dissemination of pirated content). The above classifications should be defined and included in the existing legislation to fill the vacuums.

1.10 The Computer Crimes Act, No. 24 of 2007 inherently has many deficits to be filled and reformed. As investigatory powers given under this Act are only for the prescribed crimes itemized in it, the Act cannot be applied beyond those provisions. It is a limitation on the investigatory authority of law enforcement for crimes relating to OVAC. Therefore, the act should be reviewed and reformed to allow adequate legal provisions to act upon online violence against children and women.



Establish a uniform system, structure and coordination among the relevant agencies.

Provide international training opportunities to the staff members of the cyber-crime unit of NCPA. These trainings can be obtained from the Indian Cyber Crime Coordination Center, Internet Watch Foundation UK, Federal Bureau of Investigation, the United States of America and Global Alliance Against Child Sexual Abuse Online.



2. Criminal Justice

Criminal Justice includes following sub areas

- (a) Dedicated law enforcement
- (b) Judiciary and prosecutors
- (c) Offender management process
- (d) Access to image data base.

The following recommendations can improve Sri Lankan criminal Justice process to better response to OVAC.

2.1 The Criminal Procedure Code contains some procedural laws that are not child friendly. Particularly, the police investigations which are done in a traditional manner are not equipped to provide effective responses to OVAC. Existing law enforcement procedures re-victimize the children who come in to contact with law as victims of violence. This does not ensure the best interests of the child as the child is further harmed and victimized in the justice process. Therefore, there is a need to amend relevant CPC provisions to be on par with international standards and best practices. Police Officers are bound by Departmental Orders (DOs). These DOs are not sufficiently updated to bring police investigations into a child friendly procedure. Hence, it is recommended that the DOs be amended in relation to investigations into matters pertaining to children with a special section on OVAC.

2.2 At present, there are multiple actors who play diverse roles in receiving complaints of OVAC. Therefore, a centralized system should be established to receive complaints within the law-enforcement and technical institutions. A coordination mechanism should be established among NCPA, computer crime division of the CID, SLCERT and TRC in order to effectively respond to the incidents of online violence against children.

2.3 Cyber-crimes and online violence against children often take place in global platforms which requires international cooperation. Therefore, the government of Sri Lanka (especially NCPA and CID) should initiate collaboration and coordination with international mechanisms that tackle online violence against children. This could include international mechanisms such as the Interpol, FBI, Internet Watch Foundation, NECMEC, Facebook and other technological and response mechanisms. This will also enable further technical and technological knowledge building in to local mechanisms such as Cyber Crimes/Surveillance Unit at the National Child Protection Authority.

2.4 The investigation process of the cyber-crime unit at the NCPA should be further improved by adopting new and technology based methods to investigate online violence against children. It is recommended to update the investigative methods

such as using open source VIC hash sets, custom CSAM Search Profiles, Web crawler, on-scene keyword matching, automatic classification of images and videos with AI/ML and Photo DNA. The technical advice can be obtained from SLCERT, IWF and INTERPOL.

2.5 The National Child Protection Authority and Cyber Crime Unit of the CID should work in collaboration with the Interpol to be able to get support from their international Child Sexual Exploitation data base and respond to incidents flagged by the Interpol in the country.

3. Victim support

Victim support is a critical process that should be able to effectively support victims of any form of violence including online violence. Victims support focus includes

- (a) Integrated services including after care
- (b) Child protection work force
- (c) Accessible procedures for reporting, referral and remedies
- (d) Child helpline

3.1 The National Child Protection Authority has further strengthened the National Child Helpline (1929) by the introduction of the Child Protection Mobile App, which enables children easy access to reporting incidents of online violence and risks. The law enforcement and after care (victims support unit) of the NCPA and other stakeholders must effectively and efficiently respond to the reported incidents from a victim centered approach.



Initiate collaborations with international organizations that tackle online violence against children. Such as INTERPOL, FBI and IWF. It is important for the cyber-crime unit of NCPA to collaborate with these organizations and share knowledge and technology.

3.2 Significant proportion of the children who experienced some form of online violence informed the impact lasted from few days to months, therefore psycho-social support is critical for victims of online violence. KII also revealed that serious online violence cases had long lasting psychological impact on children, and in some incidents online abuse had led to offline violence, blackmailing and commercial exploitation creating further complex issues and impact for children. Therefore psycho-social support to address issues including social norms and stigma should be provided for child victims of online violence.

3.3 Available mechanisms for other forms of violence and abuse such as case management and referral should also be utilized to provide family and community based care and protection for child victims of online violence.

3.4 High prevalence of sharing Child Sexual Abuse Materials was identified by both the children and key informants. Re-victimization and increased risks are created as a result of CSAM content being shared. Therefore, as part of the victim support the content removal should be prioritized by the authorities.

3.5 The key informant interviews revealed that the employees of the cybercrime unit of NCPA requires further training on case management, use of new technologies, softwares, storing and post management of evidence. Therefore it is recommended to provide international training opportunities to the staff of cybercrime unit. These trainings can be obtained from Indian Cyber Crime Coordination Center, Federal Bureau of Investigation, NECMEC and Global Partnership to End Violence Against Children. The State Ministry of Women and Child Development may request the support of SLCERT and Ministry of Defense in order to collaborate with the aforementioned organizations

4. Societal

Societal recommendations focus on creating an environment where violence can be prevented through support mechanisms, education and empowering children. This includes

- (a) Education programmes
- (b) Children's participation
- (c) Preventing offenders committing crimes again through offender support.

4.1 A significant proportion of the participant children proposed to include lessons on online violence

against children to formal education. Children identified Civic Studies to be the most appropriate subject for this purpose. The State Ministry of Women and Child Development and specifically NCPA could coordinate with the Ministry of Education and Higher Education to develop the curriculum. The curriculum should cover areas such as the prevalence of online violence, types of online violence, legal measures that can be taken against online violence, and methods of lodging complaints. The curriculum can be introduced to grade nine as over forty five percent of children who were interviewed in the study had first used the internet between thirteen and fifteen years of age.

4.2 Thirty two percent of the children interviewed in the study were unaware about the prevalence of online violence against children in Sri Lanka. Majority of these children were girls (nearly fifty seven percent). Children interviewed in the study identified the lack of awareness of online violence as a major factor that makes children vulnerable. Therefore, the National Child Protection Authority (NCPA), Department of Probation and Child Care Services, Children's Secretariat, private sector and civil society organisations should continue to increase awareness among children.



Introducing an educational reform to include lessons of online violence against children to the existing curriculum of civic studies and making civic studies a mandatory subject.



Conduct awareness programmes for children and parents.



Introduce online awareness programmes in collaboration with online platforms



Increase the awareness and sensitization of educators through training programmes.



Upgrade the investigation methods used by the cyber-crime unit. It is recommended to Update the investigative methods such as using open source VIC hash sets. Custom CSAM Search Profiles, on-scene keyword matching, automatic classification of images and videos with AI/ML and Photo DNA.

4.3 Understanding children's experiences and listening to their views are critically important in all settings; and children's views should be accounted in all policies and procedures as a principle approach to address online violence. Further research should be conducted to deep dive in to children's experiences on online platforms to understand risks, vulnerabilities and solutions.

4.4 NCPA, Children's Secretariat and the Department of Probation could explore the possibility of producing short instructional videos using reported cases in Sinhala and Tamil Languages. These can be played as advertisements on online platforms and at awareness raising programmes at school level.

4.5 The findings identified Facebook, Whatsapp, Messenger, Instagram, Google and YouTube to be the most frequently used online platforms by children. National Child Protection Authority and the State Ministry of Women and Child Development should request platforms such as Facebook and Google to advertise on these platforms free of charge. ICTA, SLCERT and non-governmental organizations who have the ability to connect globally can aid NCPA and the ministry to coordinate with online platforms as they already have established working relationship with platforms such as Tech- coalition.

4.6 Children identified lack of supervision by parents (64%) as a key factor that exposes children to online violence. In addition, majority of the children stated that they would not confide in a parent as they lack knowledge of online usage

and as they are afraid of further victimization by their parents.

Therefore it is important to integrate parents into awareness programmes conducted at schools and taking measures to increase the awareness of parents. The awareness programmes should enlighten parents on telltale signs of online violence, web applications and websites that are frequently used by children, working on building close relationships with children, supervising the internet usage of children without infringing on appropriate use of the internet, methods of support for victimized children, refraining from further victimization of children, taking appropriate legal action, supporting children in the post case management period and the impacts of online violence. The State Ministry of Women and Child Development should seek the support of SLCERT and ICTA to develop content.

4.7 Only a minority of children who were interviewed in the study stated that they would inform a teacher as they are afraid of victimization and breaching of confidentiality. Therefore, teachers should be provided with adequate training and information to be better skilled

in order to approach issues such as online violence. This may include ethical approaches, protecting privacy and confidentiality, creating an enabling environment to discuss issues impacting children, empathizing with victimized children, and ways by which they can provide support and referral. The NCPA should collaborate with the Ministry of Education and Higher Education, specifically with the National Institute of Education for these purposes.

5. Industry

Private sector actors including app developers, internet service providers, social media platforms and many other actors in the industry are key to effectively addressing online violence against children more than any other issue impacting children. The industry focus recommendations includes

- (a) Local removal and blocking CSAM
- (b) Reporting Child sexual abuse and exploitation
- (c) Innovative and technological solutions
- (d) Corporate social responsibility.

5.1 The findings of the study revealed that the internet service providers (ISP's) of Sri Lanka do not play a significant role in the battle against online violence. The KIs revealed that NCPA and non-governmental organizations have to go through a long legal process to gain access to phone and internet use records. As the ISPs they have a responsibility to safeguard the wellbeing of their customers, and therefore should be made a key stakeholder in the fight against online violence.



Provide secure and dedicated hardware such as technically appropriate servers, offline storing devices, computers and internet connections to the cyber-crime unit of NCPA.



NCAP should collaborate with the Telecommunication Regulatory Commission and introduce new regulations to swiftly obtain phone records and internet histories.

Therefore, it is recommended that NCPA should collaborate with the Telecommunications Regulatory Commission of Sri Lanka (TRCSL) and introduce new regulations to make ISPs responsible for supporting authorities to obtain phone records and internet usage histories more efficiently. NCPA can obtain the technical expertise of SLCERT and ICTA Sri Lanka when collaborating with TRCSL.

- 5.2 Global technological industry actors and service providers should corporate with local authorities through their in-country or regional hubs to effectively and efficiently address online violence against children, especially removing/blocking CSAM and other harmful content, pages and websites.

6. Media and Communication

Media, social media and other communication platforms can play a major role in educating, campaigning and influencing to prevent and protect children from OVAC. Similarly these platforms can also contribute to further to support vulnerable children. Media and communication should focus on

- (a) Ethical and informed media reporting and
- (b) Universal terminology

- 6.1 All stakeholders including media should use technically accurate, contextually relevant (local language) and universal terminologies in all media, communication and campaign work to ensure issues of online violence are accurately recognized in all settings.

- 6.2 65.6% of child participants believed that media does not report incidents of online violence ethically. KIs also revealed that media is sensationalizing the incidents of online violence and report inaccurately. Therefore, media personnel should be provided with training and reference materials to improve ethical reporting. NCPA should further extend their Media ethics guideline to include online violence specific areas and facilitate trainings for media personnel.

- 6.3 All child participants and key informants believed that media can play a vital role in educating, challenging social norms and sensitizing masses. Media institutions and child protection stakeholders should improve their collaboration and cooperation to use media more effectively.

The Future

The cyber-space is a rapidly transforming innovation of human technology and sense of spatiality. Especially with the Covid19 pandemic, organizations, businesses and academia across the world are demanding for more technological interventions to address the demands of the 'new normal'. It is commonsense that Sri Lanka is no exception to this. With more children are now being compelled to receive their education through online means/platforms, one cannot ignore the increase vulnerability of masses of Sri Lankan children to harmful online/cyber experiences. There is already information about pre-schools being conducted through online platforms; and this further lowers the average age of access to internet of Sri Lankan children. On the other hand it was evident through this research, while children are more susceptible/adaptable to technological innovations, the adults, educators and authorities seem to lag behind in adopting and understanding these technologies. If the recommendations of this research would fall short of being implemented, it could widen the gap between the magnitudes of the harmful cyber experiences of children and the support systems available to them in Sri Lanka.

Furthermore there are many avenues this research could not explore due to limitations and constraints. Among the key areas that need to be studied are the

implications of the Dark Web in Sri Lanka, behaviour patterns of perpetrators, violent radicalization of children and teenagers through cyber platforms, trends of self-generated explicit content, impacts of online education, and patterns of online economic activities engaged in by adolescents and youth of Sri Lanka. These areas are open for future research and it is essential that Sri Lankan authorities, organizations and industries allocate more resources towards these.

Finally, it is noteworthy to continuously re-emphasize that through this research the children of Sri Lanka have voiced up. It is their experiences, views and recommendations which have been presented in this report. Therefore it is important to listen to them and take action now, because these children are the future of Sri Lanka. All stakeholders, ranging from government authorities to civil society organizations, and ICT industries and other related industries, and academia have a shared collective responsibility to safeguard our children and to prevent all forms of online violence against children of Sri Lanka.

Bibliography

A

Aboujaoude E, Savage M, Starcevic V, et al. (2015). Online-bullying: Review of an old problem gone Viral. *J Adolesc Health*. 57, 10–18.

Alhaboby ZA, Barnes J, Evans H, Short E. (2017). Challenges facing online research: Experiences from research concerning online victimisation of people with disabilities. *Onlinepsychology* 11, 1–16.

Alvarez ARG. (2012). “IH8U”: Confronting onlinebullying and exploring the use of onlinetools in teen dating relationships.

Are you worried about online sexual abuse or the way someone has been communicating with you online? (2020), Child Exploitation and Online Protection command. Retrieved May 20th 2020 from <https://www.ceop.police.uk/safety-centre/>

Arntfield M. (2015). Towards a onlinevictimology: Onlinebullying, routine activities theory, and the anti-sociality of social media. *Can J Commun*. 40, 371–388.

Athar R. (2015). From impunity to justice: Improving corporate policies to end technology-related violence against women. *End Violence: Women's Rights and Safety Online*. Retrieved from <https://www.apc.org/en/pubs/impunity-justice-improving-corporate-policies-end-0>

Australia, S., Child Protection Systems Royal Commission, & Nyland, M. (2016). The life they deserve: Child protection systems Royal Commission Report. Government of South Australia.

Awan I, Zempi I. (2016). The affinity between online and offline anti-Muslim hate crime: Dynamics and impacts. *Aggress Violent Behav*. 27, 1–8.

B

Baek J, Bullock LM. (2014). Onlinebullying: A cross-cultural perspective. *Emotional and Behavioural Difficulties*. 19, 226–238.

Baker CK, Carreno PK. (2016). Understanding the role of technology in adolescent dating and dating violence. *J Child Fam Stud*. 25, 308–320.

Baker L, Campbell M, Barreto E. (2013). Understanding technology-related violence against women: Types of violence and women's experiences. *Learning Network, Centre for Research & Education on Violence Against Women & Children*. Retrieved from www.learningtoendabuse.ca/sites/default/files/Baker_Campbell_Barreto_Categories_Technology-Related_VAW_.pdf

Balakrishnan V. (2015). Onlinebullying among young adults in Malaysia: The roles of gender, age, and Internet frequency. *Comput Hum Behav*. 46, 149–157.

Baldasare A. (2015). Online aggression among college students: Demographic differences, predictors of distress, and the role of the University. *J Coll Student Dev*. 56, 317–330.

Baldry AC, Farrington DP, Sorrentino A. (2015). “Am I at risk of onlinebullying?” A narrative review and conceptual framework for research on risk of onlinebullying and onlinevictimization: The risks and needs assessment approach. *Aggress Violent Behav*. 23, 36–51.

Baum K, Catalano S, Rand M. (2009). Bureau of justice statistics special report: Stalking victimization in the United States. United States Department of Justice, Office of Justice Programs. Retrieved from <https://victimsofcrime.org/docs/src/baum-k-catalano-s-rand-m-rose-k2009.pdf?sfvrsn=0>

Bauman S, Pero H. (2011). Bullying and onlinebullying among deaf students and their hearing peers: An exploratory study. *J Deaf Stud Deaf Educ*. 16, 236–253.

Behav. 27, 1162–1167. Cassidy W, Faucher C, Jackson M. (2013). Onlinebullying among children: A comprehensive review of current international research and its implications and application to policy and practice. *Sch Psychol Int*. 34, 575–612.

Bennett DC, Guran EL, Ramos MC, et al. (2011). College students' electronic victimization in friendships and dating relationships: Anticipating distress and associations with risky behaviors. *Violence Vict*. 26, 410–429.

Berne S, Frisen A, Kling J. (2014). Appearance-related onlinebullying: A qualitative investigation of characteristics, content, reasons, and effects. *Body Image*. 11, 527–533.

Berne S, Frisen K, Schultze-Krumbholz S, et al. (2013). Onlinebullying assessment instruments: A systemic review. *Aggress Violent Behav*. 18, 320–334. 8 BACKE ET AL. Downloaded by Monash University package (ebook account) from www.liebertpub.com at 05/21/18. For personal use only.

Bilic V. (2013). Violence among peers in the real and virtual world. *Paediatrics Today*. 9, 78–90.

Bloom S. (2016). No vengeance for “Revenge Porn” victims: Unraveling why this latest Girls-centric, intimate-partner offense is still legal, and why we should criminalize it. *Fordham Urban Law J*. 42, 233–289.

Borrajó E, Gamez-Guadiz M, Calvete E. (2015). Online dating abuse: Prevalence, context, and relationship with offline dating aggression. *Psychol Rep*. 116, 565–585.

Bossler AM, Holt TJ, May DC. (2012). Predicting online harassment victimization among a juvenile population. *Children Soc*. 44, 500–523.

Boux HJ, Daum CW. (2015). At the intersection of social media and rape culture: How facebook postings, texting and other personal communications challenge the ‘Real’ rape Myth in the criminal justice system. *J Law Technol Policy*. 2015, 149–186.

Brochado S, Soares S, Fraga S. (2017). A scoping review on studies of onlinebullying prevalence among adolescents. *Trauma Violence Abuse*. 18, 523–531.

Brown, R., Napier, S., & Smith, R. G. (2020). Australians who view live streaming of child sexual abuse: An analysis of financial transactions. *Trends & Issues in Crime & Criminal Justice*, (589).

Burke SC, Wallen M, Vail-Smith K, et al. (2011). Using technology to control intimate partners: An exploratory study of college undergraduates. *Comput Hum*

C

Caracterización del maltrato entre iguales en una muestra de colegios de Barranquilla (Colombia). *Psicología desde el Caribe*, (16), 1–28.)

Carr, J. (2011). The Internet dimension of sexual violence against children. Council of Europe, Protecting children from sexual violence-A comprehensive approach, 281–282.

Chang F, Chiu C, Miao N, et al. (2016). Predictors of unwanted exposure to online pornography and online sexual solicitation of children. *J Health Psychol*. 21, 1107–1118.

Childhood Trends. (2017). Preventing Bullying and Online bullying: Research Based Policy Recommendations for Executive and Legislative Officials in 2017. Retrieved from <https://www.childtrends.org/wp-content/uploads/2017/01/2017-06BullyingPolicyRecsFinal.pdf> Chisholm JF. (2006). Onlinespace violence against girls and adolescent Girlss. *Ann NY Acad Sci*. 1087, 74–89.

Chisholm JF. (2014). Review of the status of onlinebullying and onlinebullying prevention. *J Inf Syst Educ*. 25, 77–87.

Choi H, Van Ouytsel J, Temple JR. (2016). Association between sexting and sexual coercion among Girls adolescents. *J Adolesc*. 53, 164–168.

Citron DK, Franks MA. (2014). Criminalizing revenge porn. *Wake Forest Law Rev*. 49, 345–391.

Citron DK. (2009). Law's expressive value in combating online gender harassment. *Mich Law Rev*. 108, 373–415.

Citron DK. (2014). Hate Crimes in Onlinespace. (Harvard University Press, Cambridge, MA.)

- Connell N, Schell-Busey NM, Pearce AN, et al. (2014). Badgrlz? exploring sex differences in online bullying behaviors. *Children Violence Juvenile Justice*. 12, 209–228.
- Craven, S., Brown S., & Gilchrist, E. (2006). Sexual grooming of children: Review of literature and theoretical considerations. *Journal of Sexual Aggression*, 12, 287–299. DOI: 10.1080/13552600601069414.
- Crimes Against Children/Online Predators (2020), Federal Bureau of Investigation, Retrieved May 20th 2020 from <https://www.fbi.gov/investigate/violent-crime/cac>
- Cutbush S, Williams J. (2016). Teen dating violence, sexual harassment, and bullying among middle school children: Examining measurement invariance by gender. *J Res Adolesc*. 26, 918–926.
- Cybercrime Convention Committee (T-CY) (2018). Working Group on cyberbullying and other forms of online violence, especially against women and children. Mapping study on cyber violence with recommendations adopted by the T-CY on 9 July 2018, France Retrieved from <https://www.coe.int/en/web/cybercrime/cyberviolence#%2250020850%22:0>
- D, Jaishankar K. (2011). Online Social Networking and Women Victims. In *Online Criminology: Exploring Internet Crimes and Criminal Behavior*.
- Davies C. (2015). Revenge porn cases increase considerably, police figures reveal. *The Guardian*. Retrieved from <https://www.theguardian.com/technology/2015/jul/15/revenge-porn-cases-increase-policefigures-reveal>
- de Vera, F. H. (2016). La construcción del concepto de paz: paz negativa, paz positiva y paz imperfecta. *Cuadernos de estrategia*, (183), 119–146.)
- Deslandes SF. (2017). Online dating abuse in affective and sexual relationships: A literature review. *Cad Sau' de Pu'blica*. 33, 1–18.
- Dick RN, McCauley JF, Jones KA, et al. (2014). Online dating abuse among teens using school-based health centers. *Pediatrics*. 134, e1560–e1567.
- Didden R, Scholte RHJ, Korzilius H, et al. (2009). Online bullying among students with intellectual and developmental disability in special education settings. *Dev Neurorehabil*. 12, 146–151.
- Dimond JP, Fiesler C, Bruckman AS. (2011). Domestic violence and information communication technologies. *Interact Comput*. 23, 413–421.
- Draft National Policy on Child Protection 2017, National Child Protection Authority, http://www.childprotection.gov.lk/?page_id=2211
- Draucker CB, Martsolf DS. (2010). The role of electronic communication technology in adolescent dating violence. *J Child Adolesc Psychiatr Nurs*. 23, 133–142.
- Dreßing H, Bailer J, Anders A, et al. (2014). Online talking in a large sample of social network users: Prevalence, characteristics, and impact upon victims. *Onlinepsychol Behav Soc Netw*. 17, 61–67.
- Drouin M, Ross J, Tobin E. (2015). A new, digital vehicle for intimate partner aggression? *Comput Hum Behav*. 50, 197–204.
- Duggan M, Rainie L, Smith A. (2014). Online harassment. Pew Research Center. Retrieved from www.pewinternet.org/2014/10/22/online-harassment/ Elípe P, de la Oliva Mun'oz M, Del Rey R. (2018). Homophobic bullying and online bullying: Study of a silenced problem. *J Homosex*. 65, 672– 686.
- E ECPAT (2009). Rio de Janeiro Declaration and Call for Action to Prevent and Stop Sexual Exploitation of Children and Adolescents
- End Revenge Porn. (2013). Revenge Porn Statistics. Online Civil Rights Initiative, Inc. Retrieved from <https://www.onlinecivilrights.org/wp-content/uploads/2014/12/RPStatistics.pdf>
- F Fascendini F, Fialova K. (2016). Voices from digital spaces: Technology related violence against women. APCWNSP. Retrieved from www.genderit.org/sites/default/upload/apcwnsp_mdg3advocacypaper_full_2011_en_0.pdf
- Faucher C, Jackson M, Cassidy W. (2014). Onlinebullying among university students: Gendered experiences, impacts, and perspectives. *Educ Res Int*. 2014, 1–10.
- Fenaughty J, Harre N. (2013). Factors associated with distressing electronic harassment and onlinebullying. *Comput Hum Behav*. 29, 803–811.
- Finchman P, Sanfilippo MR. (2015). The bad boys and girls of onlinespace: How gender and context impact perception and reaction to trolling. *Soc Sci Comput Rev*. 33, 163–180. Flach RMD,
- Fox J, Cruz C, Lee JY. (2015). Perpetuating online sexism offline: Anonymity, interactivity, and the effects of sexist hashtags on social media. *Comput Hum Behav*. 52, 436–442.
- Franklin Z. (2014). Justice for revenge porn victims: Legal theories to overcome claims of civil immunity by operators of revenge porn websites. *California Law Rev*. 102, 1303–1335.
- Franks MA. (2012). Sexual Harassment 2.0. *Md Law Rev*. 71, 655–704. Franks MA. (2015). The fight against digital abuse: The view from the US. Women's Aid. Retrieved from <https://www.womensaid.ie/16daysblog/2015/12/15/the-fight-against-digital-abuse-the-view-from-the/>
- Franks MA. (2016). "Revenge Porn" Reform: A View from the Front Lines. *Florida Law Review*. University of Miami Legal Studies Research Paper No. 16–43.
- G Gamez-Guadiz M, Almendros C, Borrajo F, et al. (2015). Prevalence and association of sexting and online victimization among spanish adults. *Sex Res Soc Policy*. 12, 145–154.
- Garett R, Lord LR, Young SD. (2016). Associations between social media and online bullying: A review of the literature. *Mhealth*. 2, 46.
- Gillespie, A.A. (2004). Grooming definitions and the law. *The New Law Journal*. 154, 586–587.
- Global Threat Assessment Report (2018), WE Protect Global Alliance, May 20th , 2020. Retrieved from <https://static1.squarespace.com/static/5630f48de4b00a75476ecf0a/tl5deecb0fc4c5ef23016423cf/1575930642519/FINAL+-Global+Threat+Assessment.pdf>
- Global Threat Assessment Report (2019), WE Protect Global Alliance, May 20th , 2020. Retrieved from <https://static1.squarespace.com/static/5630f48de4b00a75476ecf0a/tl5deecb0fc4c5ef23016423cf/1575930642519/FINAL+-Global+Threat+Assessment.pdf>
- Grant MG. (2016). In an Unsafe Space: How the rhetoric surrounding online harassment of women leaves us at risk. *Pacific Standard*. Retrieved from <https://psmag.com/news/in-an-unsafe-space> Halder
- H Hadnagy, C. (2010). Social engineering: The art of human hacking. John Wiley & Sons.
- Halder D, Jaishankar K. (2012). Online Crime and the Victimization of Women: Law, Rights and Regulations. (Information Science Reference, Hershey, PA.)
- Hamm MP, Newton A, Chisholm A, et al. (2015). Prevalence and effect of online bullying on children and young people: A scoping review of social media studies. *JAMA Pediatr*. 169, 770–777.
- Hardaker C, McGlashan M. (2016). "Real men don't hate women": Twitter rape threats and group identity. *J Pragmatics*. 91, 80–93.
- Heiman T, Olenik-Shemesh D, Eden S. (2015b). Cyberbullying involvement among students with ADHD: Related to loneliness, self-efficacy and social support. *Eur J Spec Needs Educ*. 30, 15–29.
- Heiman T, Olenik-Shemesh D. (2015a). Cyberbullying experience and gender differences among adolescents in different educational settings. *J Learn Disabil*. 48, 146–155.
- Henry N, Powell A. (2015a). Embodied harms: Gender, shame and technology-facilitated sexual violence. *Violence Against Women*. 21, 758–779.
- Henry N, Powell A. (2015b). "Beyond the "sext": Technology-facilitated sexual violence and harassment against adult women." *J Criminol*. 48, 104–118.
- Henry N, Powell A. (2016). Technology-Facilitating Sexual Violence. A Literature Review of Empirical Research. *Trauma Violence Abuse*. 19, 1–14.
- Hertz MF, David-Ferdon C. (2008). Electronic media and children violence: A CDC issue brief for educators and caregivers. Centers for Disease Control and Prevention (CDC), US Department of Health and Human Services. Retrieved from <https://www.cdc.gov/violenceprevention/pdf/ea-brief-a.pdf>
- Hinduja S, Patchin JW. (2008). Cyberbullying: An exploratory analysis of factors related to offending and victimization. *Deviant Behav*. 29, 129–156.
- Hinduja S, Patchin JW. (2010). Bullying, cyberbullying, and suicide. *Arch Suicide Res*. 14, 206–221.

Holt TJ, Fitzgerald S, Bossler AM, et al. (2016). Assessing the risk factors of cyber and mobile phone bullying victimization in a nationally representative sample of Singapore children. *Int J Offender Ther Comp Criminol*. 60, 598–615.

I INHOPE (2015). "Statistics 2014", accessed 31 March 2020, <http://www.inhope.org/tns/resources/statistics-and-infographics/statistics-and-infographics>

Internet Governance Forum (IGF) (2016). Best Practice Forum (BPF) on Online Abuse and Gender-Based Violence Against Women. Retrieved from <http://intgovforum.org/cms/documents/best-practice-forums/623bpf-online-abuse-and-gbv-against-women/file>

Inventory: An Instrument to Measure Peer Violence in Sri Lanka, BioMed Research

Is Your Child Being Cyberbullied? (2020), Web Wise Kids. Retrieved May 20th 2020 from <http://www.webwisekids.org/>

J *J Clin Psychol*. 68, 1205–1215. Ang RP. (2015). Adolescent onlinebullying: A review of characteristics, prevention and intervention strategies. *Aggress Violent Behav*. 25, 35–42.

APC Women's Rights Programme. (2015). Technology-Related Violence Against Women—A Briefing Paper. Retrieved from https://www.apc.org/sites/default/files/HRC%2029%20VAW%20a%20briefing%20paper_FINAL_June%202015.pdf

Jayarante and Rupasinghe (2015). Cyber-crime in Sri Lanka. *Journal of US-China*

Jeong S. (2015). "I'm Disappointed": Zoe Quinn Speaks Out on UN Cyberviolence Report. Motherboard. Retrieved from https://motherboard.vice.com/en_us/article/nz/7jb7/im-disappointed-zoequinn-speaks-out-on-un-cyberviolence-report

Jones LM, Mitchell KF, Finkelhor D. (2013). Online harassment in context: Trends from three children internet safety surveys (2000, 2005, 2010). *Psychol Violence*. 3, 53–69.

K K Jaishankar, ed. (CRC Press, New York, NY) pp. 758–779.

Kaye D. (2016). Promotion and protection of the right to freedom of opinion and expression. United Nations General Assembly. Retrieved from <https://digitallibrary.un.org/record/805706?ln=en>

Kaye D. (2017). UN experts urge States and companies to address online gender-based abuse but warn against censorship. United Nations Human Rights Office of the High Commissioner. Retrieved from <http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=21317&LangID=E>

Kee JS. (2005). Cultivating violence through technology? exploring the connections between internet communication technologies (ICT) and violence against women (VAW). Association of Progressive Communications Women's Networking Support Programme. Retrieved from www.genderit.org/sites/default/upload/VAW_ICT_EN.pdf

Keeping children in Sri Lanka safe and empowered online - A study on Sri Lanka's digital landscape: Potential risks to children and young people who are online, by the United Nations Children's Fund (UNICEF) Sri Lanka, Conducted by the Institute for Participatory Interaction in Development (IPID), December 2017 -<https://www.unicef.org/srilanka/reports/keeping-children-sri-lanka-safe-and-empowered-online>

King, J. E., Walpole, C. E., & Lamon, K. (2007). Surf and turf wars on line: Growing implications of Internet gang violence. *Journal of Adolescent Health*, 41, S66–S68

King-Ries A. (2008). Teens, Technology and Cyber stalking: The Domestic Violence Wave of the Future? *Tex J Women Law*. 20, 131–164.

Kiriakidis SP, Kavoura A. (2016). Cyberbullying: A review of the literature on harassment through the internet and other electronic means. *Fam Community Health*. 33, 82–93.

Kowalski RM, Giumetti GW, Schroeder AN, et al. (2014). Bullying in the digital age: A critical review and meta-analysis of cyberbullying research among children. *Psychol Bull*. 140, 1073–1137.

Kowalski RM, Limber SP, Agatson P. (2012). *Cyberbullying in the Digital Age*. (Wiley-Blackwell, Oxford.)

Kowalski RM, Morgan CA, Drake-Lavelle K, et al. (2016). Cyberbullying among college students with disabilities. *Comput Hum Behav*. 57, 416–427.

Krieger MA. (2017). Unpacking "sexting": a systematic review of nonconsensual sexting in legal, education, and psychological literatures. *Trauma Violence Abuse*. 18, 593–601.

L Larkin PJ. (2015). Revenge porn, state law, and free speech. *Loyola Los Angeles Law Rev*. 48, 57–118.

Laxton C. (2014). Virtual World, Real Fear: Women's Aid report into online abuse, harassment and stalking. Women's Aid. Retrieved from <https://www.womensaid.org.uk/virtual-world-real-fear/>

Lenhart A, Ybarra M, Zickuhr K, et al. (2016). Online Harassment, Digital Abuse, and Cyberstalking in America. Data & Society. Retrieved from https://www.datasociety.net/pubs/oh/Online_Harassment_2016.pdf

Lindsay M, Booth JM, Messing JT, et al. (2015). Experiences of online harassment among emerging adults: Emotional reactions and the mediating role of fear. *J Interpers Violence*. 31, 1–22.

Lindsay M, Krysiak J. (2016). Online Harassment Among College Students: A replication incorporating new Internet trends. *Inf Commun Soc*. 1, 703–719.

Livingstone, S., & Haddon, L. (2009). EU Kids Online: final report/LSE, London: EU Kids Online. EC Safer Internet Plus Programme Deliverable D, 6.

Llorent VJ, Ortega-Ruiz R, Zych I. (2016). Bullying and cyberbullying in minorities: Are they more vulnerable than the majority group? *Front Psychol*. 7, 1507.

Luckman S. (1999). (En) gendering the digital body: Feminism and the Internet. *Hecate*. 25, 36–47.

M Mantilla K. (2015). *Gendertrolling: How Misogyny Went Viral*. (Praeger, Denver, CO.)

Marcum CD, Higgins GE, Nicholson J. (2017). I'm watching you: Cyberstalking behaviors of university students in romantic relationships. *Am J Criminal Justice*. 42, 373–388.

Marcum CD, Higgins GE, Ricketts ML. (2014). Juveniles and cyber stalking in the United States: An analysis of theoretical predictors of patterns of online perpetration. *Int J Cyber Criminol*. 8, 47–56.

Marganski A, Melander L. (2018). Intimate partner violence victimization in the cyber and real world: Examining the extent of cyber aggression experiences and its association with in-person dating violence. *J Interpers Violence*. 33, 1071–1095.

Marret MJ, Choo WY. (2017). Factors associated with online victimization among Malaysian adolescents who use social networking sites: A cross-sectional study. *BMJ Open*. 7, e014959.

Matsui S. (2015). The Criminalization of revenge porn in Japan. *Washington Int Law J*. 24, 289–317.

McCue C. (2016). Ownership of Images: The Prevalence of Revenge Porn Across a University Population. (Bridgewater, MA: Bridgewater State University).

McGlynn C, Rackley E, Houghton R. (2017b). "Beyond Revenge Porn": The continuum of image-based sexual abuse. *Feminist Leg Stud*. 25, 25–46.

McGlynn C, Rackley E. (2017a). Image-based sexual abuse. *Oxford J Leg Stud*. 37, 534–561.

Megarry J. (2014). Online incivility or sexual harassment? Conceptualizing women's experiences in the digital age. *Womens Stud Int Forum*. 47, 46–55.

Melander LA. (2010). College students' perceptions of intimate partner cyber harassment. *Cyberpsychol Behav Soc Netw*. 13, 263–268.

Mishna F, Cook C, Siani M, et al. (2011). Interventions to prevent and reduce cyber abuse of children: A systematic review. *Res Soc Work Pract*. 21, 5–14.

Mishna F, McLuckie A, Saini M. (2009). Real-world dangers in an online reality: A qualitative study examining online relationships and cyber abuse. *Soc Work Res*. 33, 108–118.

Mitchell KJ, Finkelhor D, Wolak J, et al. (2011). Children internet victimization in a broader victimization context. *J Adolesc Health*. 48, 128–134.

Mitchell KJ, Ybarra ML, Jones LM, et al. (2016). What features make online harassment incidents upsetting to children? *J Sch Violence*. 15, 279–301.

Montiel I, Carbonell E, Pereda N. (2016). Multiple online victimization of Spanish adolescents: Results from a community sample. *Child Abuse Negl*. 52, 123–134.

Morelli M, Bianchi D, Baiocco R, et al. (2016). Sexting, psychological distress and dating violence among adolescents and young adults. *Psicothema*. 28, 137–142.

MTV, Associated Press. (2011). *Executive Summary: 2011 AP-MTV Digital Abuse Study. A Thin Line*. Retrieved from www.athinline.org/pdfs/MTV-AP_2011_Research_Study-Exec_Summary.pdf

N

Normand CL, Sallafranque-St-Louis F. (2016). Cybervictimization of young people with an intellectual or developmental disability: Risks specific to sexual solicitation. *J Appl Res Intellect Disabil*. 29, 99–110.

O

O'Connell, R. (2003). A typology of child cyberexploitation and online grooming practices. Retrieved from <http://image.guardian.co.uk/sysfiles/>

Ojanen TT, Boonmongkon P, Samakkeekarom R, et al. (2015). Connections between online harassment and offline violence among children in Central Thailand. *Child Abuse Negl*. 44, 159–169.

Open Democracy (2017), *Investigating Sri Lanka's 'nude'*

P

Paasonen S. (2011). Revisiting cyberfeminism. *Communications*. 36, 335–352.

Patchin JW, Hinduja S. (2012). *Cyberbullying Prevention and Response: Expert Perspectives*. (Routledge, New York, NY.)

PEaCE/IECPAT . 2017. *Protecting Environment and Children Everywhere Alternative Report*, PEaCE/IECPAT Sri Lanka and ECPAT International, Colombo, Sri Lanka

Peskin MF, Markham CM, Shegog R, et al. (2017). Prevalence and correlates of the perpetration of cyber dating abuse among early adolescents. *J Children Adolesc*. 46, 358–375.

Phillips W. (2015). *This Is Why We Can't Have Nice Things: Mapping the Relationship Between Online Trolling and Mainstream Culture*. (MIT Press, Cambridge, MA.)

Picard P. (2007). *Tech Abuse in Teen Relationships Study*. Liz Claiborne, Inc. Retrieved from www.loveisrespect.org/wp-content/uploads/2009/03/liz-claiborne-2007-tech-relationship-abuse.pdf

Pittaro ML (2011). *Cyberstalking: Typology, etiology and victims*. In *Cyber Criminology: Exploring Internet Crimes and Criminal Behavior*. K Jaishankar, ed. (CRC Press, New York, NY) pp. 277–297.

Powell A. (2010). Configuring consent: Emerging technologies, unauthorized sexual images and sexual assault. *Aust N Z J Criminol*. 43, 76–90.

Priebe G, Mitchell KJ, Finkelhor D. (2013). To tell or not to tell? Children's responses to unwanted Internet experiences. *Cyberpsychology*. 7, 71–84.

Public Administration, 12(10), pp 759-763

R

Rainie L, Wellman B. (2012). *Networked: The New Social Operating System*. (MIT Press, Cambridge, MA.)

Razak, A. (2018 May 13). Internet connections rise 20% in 2017. *The Sunday Observer*. Retrieved from <http://www.sundayobserver.lk/2018/05/13/news/internet-connections-rise-20-2017>

Redondo-Sama G, Pulido-Rodriguez MA, Lerna R, et al. (2014). Not without them: The inclusion of Minors' voices on cyber harassment prevention. *Qual Inq*. 20, 895–901.

Reed LA, Tolman RM, Ward LM. (2016). Snooping and sexting: Digital media as a context for dating aggression and abuse among college students. *Violence Against Women*. 22, 1556–1576.

Reed LA, Tolman RM, Ward LM. (2017). Gender matters: Experiences and consequences of digital dating abuse victimization in adolescent dating relationships. *J Adolesc*. 59, 79–89.

Reyns BW, Henson B, Fisher BS. (2011). Being pursued online: applying cyberlifestyle-routine activities theory to cyberstalking victimization. *Crim Justice Behav*. 38, 1149–1169.

Reyns BW, Henson B, Fisher BS. (2012). Stalking in the twilight zone: Extent of cyber stalking victimization and offending among college students. *Deviant Behav*. 33, 1–25.

Reyns BW, Henson B, Fisher BS. (2016). Guardians of the cyber galaxy: An empirical and theoretical analysis of the guardianship concept from routine activity theory as it applies to online forms of victimization. *J Contemp Criminal Justice*. 32, 148–168.

Runions KC, Bak M. (2015). Online moral disengagement, cyberbullying, and cyber-aggression. *Cyberpsychol Behav Soc Netw*. 18, 400–405.

S

Sabella RA, Patchin JW, Hinduja S. (2016). Cyberbullying myths and realities. *Comput Hum Behav*. 29, 2703–2711.

Sargent KS, Krauss A, Jouriles EN, et al. (2016). Cyber victimization, psychological intimate partner violence, and problematic mental health outcomes among first-year college students. *Cyberpsychol Behav Soc Netw*. 19, 545–550.

Selkie EM, Fales JL, Moreno MA. (2016). Cyberbullying prevalence among US middle and high-school aged adolescents: A systematic review and quality assessment. *J Adolesc Health*. 58, 125–133.

Shahani A. (2014). *Smartphones Are Used to Stalk, Control Domestic Abuse Victims*. All Tech Considered: NPR. Retrieved from www.npr.org/sections/alltechconsidered/2014/09/15/346149979/smartphones-are-used-to-stalk-control-domestic-abuse-victims

Shimizu A. (2013). Domestic violence in the digital age: Towards the creation of a comprehensive cyberstalking statute. *Berkeley J Gender Law Justice*. 28, 116–137.

Smith PK, Mahdavi J, Carvalho M, et al. (2008). Cyberbullying: Its nature and impact on secondary school pupils. *J Child Psychol Psychiatry*. 49, 376–385.

Smith PK, Thompson F, Davidson J. (2014). Cyber safety for adolescent girls: Bullying, harassment, sexting, pornography, and solicitation. *Obstet Gynecol*. 26, 360–365.

Smith PK. (2012). Cyberbullying and cyber aggression. In *Handbook of School Violence and School Safety*. SJ Jimerson, AB Nickerson, MJ Mayer, MJ Furlong, eds. (Routledge, New York) pp. 93–103.

Smith-Darden JP, Kernsmith PD, Victor BG, Lathrop RA. (2017). Electronic displays of aggression in teen dating relationships: Does the social ecology matter? *Comput Hum Behav*. 67, 33–40. Stoleru M, Costescu E. (2014). (Re) Producing Violence Against Women in Online Spaces. *Philobiblon XIX*. 95–114.

Sri Lanka Research Report: The sexual abuse, commercial sexual exploitation and trafficking of children in Sri Lanka (December 2008), Swiss Solidarity and SAPSRI, Jason Squire and Sarasi Wijeratne, http://www.iccnwspcanarc.org/upload/pdf/8389414843trafficking_report_srilanka_17_12_08.pdf and <http://lastradainternational.org/doc-center/2082/sri-lanka-research-report-the-sexual-abuse-commercial-sexual-exploitation-and-trafficking-of-children-in-sri-lanka>

Stoltenborgh, M., Van Ijzendoorn, M. H., Euser, E. M., & Bakermans-Kranenburg, M. J. (2011). A global perspective on child sexual abuse: meta-analysis of prevalence around the world. *Child maltreatment*, 16(2), 79–101.

Stonard KE, Bowen E, Lawrence TR, et al. (2014). The relevance of technology to the nature, prevalence and impact of Adolescent Dating Violence and Abuse: A research synthesis. *Aggress Violent Behav*. 19, 390–417.

Strawhun J, Adams N, Huss MT. (2013). The assessment of cyber stalking: An expanded examination including social networking, attachment, jealousy, and anger in relation to violence and abuse. *Violence Vict*. 28, 715–730.

Stroud SR. (2014). The dark side of the online self: A pragmatist critique of the growing plague of revenge porn. *J Mass Media Ethics*. 29, 168–183.

Subrahmanyam, K., Garcia, E. C., & Harsono, L. S. (2009). In their words: Connecting online weblogs to developmental processes. *British Journal of Developmental Psychology*, 27, 219–245.

Subrahmanyam, K., Smahel, D., & Greenfield, P. (2006). Connecting developmental constructions to the Internet: Identity presentation and sexual exploration in online teen chat rooms. *Developmental Psychology*, 42, 395–406.

Sullivan J. (2009). Professionals who sexually abuse the children with whom they work. Unpublished Ph.D. Thesis, School of Psychology, University of Birmingham.

Sullivan, J., and Quayle, E. (2012). *Manipulation Styles of Abusers who Work with Children in M. Erooga (Ed) Creating Safer Organisations: Practical Steps to Prevent the Abuse of Children by Those Working with Them*, Wiley & Sons, Ltd, London.

Sumner, S.A., Mercy, J.A., Saul, J., Motsa-Nzuza, N., Kwesigabo, G., Buluma, R., ... & Kilbane, T. (2015). Prevalence of sexual violence against children and use of social services—seven countries, 2007–2013. *MMWR. Morbidity and mortality weekly report*, 64(21), 565.

Sun S, Fan X, Du J. (2016). Cyberbullying perpetration: A metaanalysis of gender differences. *Int J Internet Sci*. 11, 61–81.

T Temple JR, Choi HF, Brem M, et al. (2016). The temporal association between traditional and cyber dating abuse among adolescents. *J Children Adolesc*. 45, 340–349.

Tennakoon et al (2018). Child Online Safety and Parental Intervention: a study of Sri Lankan internet users, *Information Technology & People*, 31(03)

The Economist Intelligence Unit. 2018. Out of the shadows: Shining light on the response to child sexual abuse and exploitation- a 40 country benchmarking index. Sri Lanka country summary. EIU, New York, NY.

Tokunaga RS, Aune KS. (2017). Cyber-defense: A taxonomy of tactics for managing cyberstalking. *J Interpers Violence*. 32, 1451–1475.

Tokunaga RS. (2010). Following you home from school: A critical review and synthesis of research on cyberbullying victimization. *Comput Hum Behav*. 26, 277–287.

U UN Broadband Commission for Digital Development Working Group on Broadband and Gender. (2015). Cyber violence against women and girls: A world wide wake-up call. United Nations. Retrieved from www.broadbandcommission.org/Documents/reports/bb-wggender-discussionpaper2015-executive-summary.pdf

UN General Assembly, Article 19, Convention on the Rights of the Child. www.ohchr.org/en/professionalinterest/pages/crc.aspx

Understanding the Megan Meier Case. (2020, March 21). <https://cyber.laws.com/megan-meier-case>

Understanding the Megan Meier Case. (2020, March 21). <https://cyber.laws.com/megan-meier-case>

UNICEF, 2017, Keeping Children In Sri Lanka Safe and Empowered Online - A study on Sri Lanka's landscape: Potential risks to children and young people who are online", Colombo. Sri Lanka

United States Department of Justice. (2001). Stalking and domestic violence: Report to congress. Office of Justice Programs, Violence Against Women Office. Retrieved from <https://www.ncjrs.gov/pdffiles1/ojp/186157.pdf>

V Van der Gaag N. (2010). Because I am a Girl: The State of the World's Girls 2010—Digital and Urban Frontiers: Girls in a Changing Landscape. Plan. Retrieved from www.citiesalliance.org/sites/citiesalliance.org/files/BIAAG_2010_EN2.pdf

Van Ouytsel J, Ponnet K, Walrave M, et al. (2016). Adolescent cyber dating abusive victimization and its association with substance use and sexual behaviors. *Public Health*. 135, 147–151.

Van Ouytsel J, Torres E, Choi HJ, et al. (2017). The associations between substance use, sexual behaviors, bullying, deviant behaviors, health, and cyber dating abuse perpetration. *J Sch Nurs*. 33, 116–122.

Van Ouytsel J, Walrave M, Ponnet K. (2015). The association between adolescent sexting, psychosocial difficulties, and risk behavior: integrative review. *J Sch Nurs*. 31, 54–69.

Van Wilsem J. (2013). Hacking and harassment—Do they have something in common? comparing risk factors for online victimization. *J Contemp Criminal Justice*. 29, 437–453.

Vivolo-Kanto AM, Martell BN, Holland KM, et al. (2014). A systematic review and content analysis of bullying and cyber-bullying measurement strategies. *Aggress Violent Behav*. 19, 423–434.

W Wachs S, Whittle HC, Hamilton-Giachritsis C, et al. (2018). Correlates of mono- and dual-victims of cybergrooming and cyberbullying: Evidence from four countries. *Cyberpsychol Behav Soc Netw*. 21, 91–98.

Wajcman J. (2010). Feminist theories of technology. *Cambridge J Econ*. 34, 1430152.

Walker K, Sleath E. (2017). A systematic review of the current knowledge regarding revenge pornography and non-consensual sharing of sexually explicit media. *Aggress Violent Behav*. 36, 9–24.

Weinstein EC, Selman RL. (2016). Digital stress: Adolescents' personal accounts. *New Media Soc*. 18, 391–409.

Wells M, Mitchell KF. (2014). Patterns of internet use and risk of online victimization for children with and without disabilities. *J Spec Educ*. 48, 204–213.

West J. (2016). Cyber-violence against women. Battered Women's Support Services. Retrieved from www.bwss.org/wp-content/uploads/2014/05/CyberVAWReportJessicaWest.pdf

Wijeratne et al (2014). Development of the Sri Lankan Early Teenagers' Violence

Wingate VS, Minney JA, Guadagno RE. (2013). Sticks and stones may break your bones, but words will always hurt you: A review of cyberbullying. *Soc Influence*. 8, 87–106.

Wolak J, Finkelhor D, Mitchell KJ, et al. (2010). Online "Predators" and their victims: Myths, realities, and implications for prevention and treatment. *Psychol Violence*. 1, 13–35.

Wolak J, Mitchell KJ, Finkelhor D. (2007). Does online harassment constitute bullying? An exploration of online harassment by known peers and online-only contacts. *J Adolesc Health*. 41, S51–S58.

Wolford-Clevenger C, Zapor H, Brasfield H, et al. (2016). An examination of the partner cyber abuse questionnaire in a college student sample. *Psychol Violence*. 6, 156–162.

Woodlock D. (2016). The Abuse of Technology in Domestic Violence and Stalking. *Violence Against Women*. 31, 3174–3195.

Working to Halt Online Abuse (WHOA) (2011). Online harassment/ cyberstalking statistics. Working to Halt Online Abuse (WHOA). Retrieved from www.haltabuse.org/resources/stats/

Working to Halt Online Abuse (WHOA) (2011). Online harassment/ cyberstalking statistics. Working to Halt Online Abuse (WHOA). Retrieved from www.haltabuse.org/resources/stats/

Wright MF. (2017). Parental mediation, cyberbullying and cyberstalking: The role of gender. *Comput Hum Behav*. 71, 189–195.

Wright, MF. (2015). Cyber aggression within adolescents' romantic relationships: Linkages to parental and partner attachment. *J Children Adolesc*. 44, 37–47.

Y Yahner J, Dank M, Zweig JM. (2015). The co-occurrence of physical and cyber dating violence and bullying among teens. *J Interpers Violence*. 30, 1079–1089.

Ybarra ML, Boyd D, Korchmaros JD, et al. (2012). Defining and measuring cyberbullying within the larger context of bullying victimization. *J Adolesc Health*. 51, 53–58.

Ybarra ML, Espelage D, Mitchell KF. (2007). The co-occurrence of internet harassment and unwanted sexual solicitation victimization and perpetration: Associations with psychosocial indicators. *J Adolesc Health*. 41, S31–S41.

Young A, Young A, Fullwood H. (2007). Adolescent online victimization. *Prev Res*. 14, 8–9. Zerach G. (2016). Pathological narcissism, cyberbullying victimization and offending among homosexual and heterosexual participants in online dating websites. *Comput Hum Behav*. 57, 292–299.

Z Zweig JM, Dank M, Lachman P, et al. (2013a). Teen Dating Violence and Abuse, and Bullying. (Washington, DC: Urban Institute, Justice Policy Center).

Zweig JM, Dank M, Yahner J, et al. (2013b). The rate of cyber dating abuse among teens and how it relates to other forms of teen dating violence. *J Children Adolesc*. 42, 1063–1077.

Zweig JM, Lachman P, Yahner J. (2014). correlates of cyber dating abuse among teens. *J Children Adolesc*. 43, 1306–1321.

Zych I, Ortega-Ruiz R, Rey RD. (2015). Scientific research on bullying and cyberbullying: Where have we been and where are we going. *Aggress Violent Behav*. 24, 188–298.

Annex 01



Research on the incidence, nature and scope of online violence against children, and the mechanisms that respond to cases of online violence against children Social Policy Analysis and Research Centre (SPARC) University of Colombo

This is a questionnaire, to be administered face-to-face to children aged 13-17 at home. This is part of the Research on the incidence, nature and scope of online violence against children, and the mechanisms that respond to cases of online violence against children.

The questionnaire examines how children and young people engage with the internet and online or digital technologies in their everyday lives. It has been developed by Social Policy Analysis and Research Centre (SPARC) based on work by EU Kids Online (EUKO).

Eligibility criteria

For the enumerators: The respondent is eligible to participate in the survey only if she or he is using internet. Using internet refers to the use of any of the following. If the answer is "NO" thank the respondents and explain that according to the requirements of the survey he or she cannot participate.

Do you use internet? Yes ☐ No ☐

Facebook	Instagram	twitter	imo	Viber	Watts app	Pinterest	Messenger
WeChat	Tik Tok	Google	Yahoo!	Gmail	Y MAIL	PUBG	Online games
Snap Chat	You Tube	Skype	Chrome	Mozilla	Windows Explorer	Safari	Face Time/ Duo

INTERVIEWER'S ACCOUNT – DO NOT ASK RESPONDENT**INTERVIEWER: FILL IN AT THE END OF INTERVIEW**

Date of interview:

DD	MM	YYYY
----	----	------

Time

HH	MM
----	----

Length of interview:

(in minutes)	Mins
--------------	------

Gender of interviewer:

--

Please note that the interviewer is obligated to inform to the team leader and the child safeguarding focal point of the research staff if the child is found to be vulnerable or subjected to any form of online abuse.

- Who was in the room when the CHILD FACE-TO-FACE interview took place?

The parent	1
Guardian	2
No one else	3

- Who was in the room when the CHILD COMPLETED THE SELF-COMPLETION SECTIONS?

The parent	1
Guardian	2
No one else	3

Section A: Child identity and resources (Part 1)**Introduction**

I am going to start with some questions about you, if that's okay. If I ask a question that you don't want to answer at any point, just tell me and we'll skip that question. If you don't know or don't want to answer any of the questions, just say so. And do ask me if you don't understand something.

01. Record if the child is a boy, a girl, or other. If unsure, can ask: What is your gender?

Male	Female	Other (Pls Specify)
1	2	3

02. How old are you?

--

03. Thinking about the home where you live all or most of the time, tell us all the people who live there.
(Multiple response question)

Male	Female	Step Father	Step Mother	Grand Parents	Other relatives	Alone	Other (Pls Specify)
1	2	3	4	5	6	7	8

Education

04. Which of these things apply to you? (Multiple Response)

I am schooling	I am a student in vocational training	Other (Pls Specify)
1	2	3

05. What is the highest level of formal education (in years)

.....
.....
.....

Cultural origin

06. What is your ethnicity?

Sinhalese	Sri Lankan Tamil	Upcountry Tamil	Muslim	Burger	Other (Pls Specify)
1	2	3	4	5	6

07. What is your religion?

Buddhist	Hindu	Islam	Roman Catholic	Christian (Non Roman Catholic)	Other (Pls Specify)
1	2	3	4	5	6

Section B: Behaviour on social networking sites

























Now I would like to ask you about social networking. By this we mean sites e.g., Facebook or Instagram] where you can have a profile and where you can keep in touch with people and share things with them.

Online practices













08. Which of these activities do you do when you use internet (Rank in order)?
Multiple Response Question

Learning News Skill Development	Connecting With peers	Developing creative skills	Watching videos	Listening to music	Making models	Online Gaming	Making Money	Other (Pls Specify)
1	2	3	4	5	6	7	8	

09. Which websites or apps do you mostly use these days? (Rank in order – according the frequency of use)

							
Facebook	Instagram	twitter	imo	Viber	Watts app	Pinterest	Messenger
							
WeChat	Tik Tok	Google	Yahoo!	Gmail	Y MAIL	PUBG	Online games
							
Snap Chat	You Tube	Skype	Chrome	Mozilla	Windows Explorer	Safari	Face Time/ Duo

Please look at the social media sites given below and answer the following questions

					
Facebook	Instagram	twitter	imo	Viber	Watts app
					
Pinterest	Messenger	WeChat	Tik Tok	Snap Chat	PUBG

10. Do you have your own profile on a social networking or social media or gaming site that you currently use?

Yes	No
1	2

11. How many profiles do you have on the same site ?

Social networking site	Number of profiles
Facebook	
Instagram	

Twitter	
Watts App	
Messenger	
Imo	
Viber	
Other (Pls Specify)	
Q.21 Total number of profiles	

12. Thinking of the profile you use most often, about how many people are you in frequent communication with when using [most used profile]?

.....
.....
.....

Section C: Prevalence of Online violence against children

Now I am going to ask few questions about your experiences of cyber violence. Refer to the guidelines for a detailed definition of online violence.

13. Have you heard about online violence against children?

Yes	No
1	2

14. Would you identify any of the following as an online violence against children?

Scenario	Yes	No
Sending an indecent text messages		
Sending an indecent picture/clipart/video/text/script/audio clips/emails		
Sharing indecent picture/clipart/video/text/script/audio clips/emails		
Cyber Bullying (example: harassing or threatening or making abusive fun of some one using electronic means)		
Cyber Extortion		
Other (Pls Specify)		

ATTENTION: Research Assistants/Enumerators – Please kindly allow the child to fill in the self-administered questionnaire now. Please allocate 20 minutes to complete the self-administered questionnaire.

Whence the child has completed the self-administered questionnaire you can resume the face-to-face interview from the question No.15 given below.

15. Do you think that there are laws and rules available for the protection of children in Sri Lanka?

Yes	No
1	2

16. If you become a victim of cyber violence in the future, would you make a complaint to take legal action against the perpetrators?

Yes	No
1	2

17. If the answer is “Yes” to which organization would you lodge a complaint?

Sri Lanka Police	SLCERT	NCPA	Other (Pls Specify)
1	2	3	4

18. If the answer is “No” why wouldn’t you take action?

.....
.....
.....
.....
.....
.....

19. Have any of your friend/friends experienced any of the above mentioned forms of violence?

Yes	No
1	2

20. If yes, what are those forms of violence?

Online bullying	Engaging in sexual activities online	Revenge Porn	Child pornography	Cyber stalking	Identity theft	Online grooming	Any other
1	2	3	4	5	6	7	

21. Can you briefly explain the forms of violence they experienced?

.....
.....
.....
.....
.....
.....

22. Did they take any legal action against it?

Yes	No
1	2

22. (a) If the answer is “Yes” to which organizations did they complain?

Sri Lanka Police	SLCERT	NCPA	Any other (Pls Specify)	Not applicable
1	2	3	4	0

(b) If they did not take legal action are you aware of the reason behind their decision.

Yes	No
1	2

(c) Can you briefly explain the reasons if you know?

.....
.....
.....

23. According to your opinion do parents have a knowledge on cyber violence?

Yes	No
1	2

24. Are the parents aware of the legal mechanisms available for child's protection against cyber violence?

Yes	No
1	2

25. Do parents consider cyber violence to be a serious issue?

Yes	No
1	2

26. Have your parents have had a discussion with you about cyber violence?

Yes	No
1	2

26. (a) If the answer is yes what did you and your parents talk about?

.....
.....
.....
.....
.....

27. If you experienced cyber violence what was your parent's reaction if you informed the incident to them?

Supported you in complaining to the authorities	Listened to you but did not take any action	Listened to you and advised you not to take any action	Listened briefly and Blamed you	Did not listen to you or take any action	Listened to you and took the device away	Any other (Pls Specify)
1	2	3	4	5	6	7

28. Do you think the educators (teachers, principals, Counsellors) have a good understanding about cyber violence?

Yes	No
1	2

29. How would you think the educators will handle the complaint?

Supported you in complaining to the authorities	Listened to you but did not take any action	Listened to you and advised you not to take any action	Listened briefly and Blamed you	Did not listen to you or take any action	Any other (Pls Specify)
1	2	3	4	5	6

30. If you experience a cyber-violence will you discuss this with an educator?

Yes	No
1	2

31. If the answer is yes please clarify your answer

.....
.....
.....
.....
.....

32. If the answer is NO please clarify your answer.

.....
.....
.....
.....
.....

33. Do you think the mobile service providers have a sound understanding of cyber violence?

Yes	No
1	2

34. According to you have the service providers taken enough measures to curb and discourage cyber violence against children?

Yes	No
1	2

35. If the answer is yes can you please name few of these measures?

.....
.....
.....
.....
.....

36. Do you think Sri Lankan Mass media has a good knowledge of online violence against children?

Yes	No
1	2

37. If the answer is “Yes” can you please clarify your answer?

.....
.....
.....
.....
.....

38. According to you which of the following media outlets pay better attention to cyber violence against children?

Government Television Channels	Private Television Channels	Radio Channels	Newspapers	New media outlets such as YouTube	Any other
1	2	3	4	5	6

39. Do you think the way the media is handling the issue is appropriate?

Yes	No
1	2

40. If “Yes” please clarify your answer?

.....
.....
.....
.....
.....

41. If “No” please clarify the answer.

.....
.....
.....
.....
.....

42. According to you what factors make some children more vulnerable to online violence?

Lack of awareness On cyber violence	Lack of supervision by parent	Sharing personal information publicly	Trusting people you meet on line too much	Other factor	Other factor
1	2	3	4	5	6

43. How do you think the impact of these factors can be reduced?

By increasing awareness	By increasing the awareness of the parents guardians	Teaching about cyber violence at school	Introducing online reporting methods	By introducing harsher punishments for perpetrators	By giving more power to the organizations responsible for child protection	Other answer
1	2	3	4	5	6	7

44. According to you how the online violence against children can be prevented?

By increasing awareness	By increasing introducing tools that can block unnecessary people online	Teaching about cyber violence at school	By increasing parents supervision	By introducing harsher punishments for perpetrators	By giving more power to the organizations responsible for child protection	Other
1	2	3	4	5	6	7

45. According to your opinion what type of support children need to be safe from cyber-violence ?

Paying attention to what children has to say about online violence	Introducing more user-friendly reporting services by the internet Service providers	Introducing harsher punishments for perpetrators	Giving more power to the organizations responsible for child protection	Other answer (Pls Specify)	Other answer (Pls Specify)
1	2	3	4	5	6

46. Please further clarify your answer

.....
.....
.....
.....
.....

47. According to you what type of support children need when they are faced with online violence?
(Multiple response Question – Choose all applicable).

Psychological support	Legal support	Psychosocial support	Other answer	Other answer	Other answer
1	2	3	4	5	6

48. According to you which ones of the above mentioned support methods are the most important? Rank in order

Psychological support	Legal support	Psychosocial support	Other answer	Other answer	Other answer

49. Kindly clarify your answer

50. How would you prefer to receive the mentioned support?

51. Would you like to say anything else about online violence that we have not covered in this questionnaire?

Section D: Access

People use the internet differently, so let's now talk about how you use it. Think about all the different ways you might use the internet, such as emailing, visiting website, or chatting with your friends [please refer to the list given in the first page of the questionnaire].

52. How old were you when you first used the internet?

.....

53. How often do you use the internet?

Hardly ever	At least once in every month Monthly/At least once a month	At least once in every week/ weekly/at least once a week	Daily or almost daily	Several times each day	Almost all the time	Other (Pls Specify)
1	2	3	4	5	6	7

54. Are you able to access the facilities to use the internet when you need?

Never	Sometimes	Often	All the time
1	2	3	4

55. Are you able to access the facilities to use the internet when you want to ?

Never	Sometimes	Often	All the time
1	2	3	4

56. How often do you go online or use the internet at the following places?

a. At school or college

Never	Hardly ever	At least once in every month	At least once every week	At least once every day Daily or almost daily	Several times each day	All the time	Other (Pls Specify)
1	2	3	4	5	6	7	8

b. At home

Never	Hardly ever	At least once in every month	At least once every week	Daily or almost daily	Several times each day	All the time	Other (Pls Specify)
1	2	3	4	5	6	7	8

c. At the homes of relatives

Never	Hardly ever	At least once in every month	At least once every week	Daily or almost daily	Several times each day	All the time	Other (Pls Specify)
1	2	3	4	5	6	7	8

d. At the homes of friends ?

Never	Hardly ever	At least once in every month	At least once every week	Daily or almost daily	Several times each day	All the time	Other (Pls Specify)
1	2	3	4	5	6	7	8

e. In a public place (for example, in libraries, cafes and restaurants, free-wifi-zones)

Never	Hardly ever	At least once in every month	At least once every week	Daily or almost daily	Several times each day	All the time	Other (Pls Specify)
1	2	3	4	5	6	7	8

f. How much time do you spend on online platforms during their travel time?

.....
.....
.....
.....
.....

57. What devices do you use to access internet?

A mobile phone that is not a smartphone	A smartphone	Desktop computer	A laptop or notebook computer	A tablet	Smart watch	Gaming console	Other (Pls Specify)
1	2	3	4	5	6	7	8

Section E: Connectivity and Technological Safety Measures in Social Media Usage

58. When you use the internet, how do you connect?

I use prepaid internet (e.g post-paid internet/wifi data/mobile data/home wifi/ hotspots)	I use free internet (e.g., in school, cafes, libraries, other people's devices)	I go somewhere where I can pay for internet each time I use it (e.g., in a cybercafé, public pay-to-use computers)	Other (Pls Specify)
1	2	3	

Time spent online

59. How long do you spend on the internet on an ordinary weekday (school day or working day)?

.....
.....
.....
.....
.....

60. About how long do you spend on the internet on a day at the weekend and a holiday?

.....
.....
.....
.....
.....

Tech-based Safety Measures in Social Media Usage

61. Is your profile set to...?

Public, so that everyone can see it	Partially private, so that friends of friends or my networks can see	Private, so that only my friends can see
1	2	3

62. Which of these kinds of information does your [named] profile show about you?

A photo that clearly shows your face	Real name	Your last name	Your address	Your phone number	Your correct age	Your relationship status	Information of your family
1	2	3	4	5	6	7	8

63. (a) How do you usually respond to requests from people to become your 'friends' online?

I usually accept all requests	I accept only if we have friends in common	I accept only if I have met them in person	I accept only if I have met them multiple times in close peer circles very well
1	2	3	4

(b) Can you please explain the answer you gave to Q 63 a ?

64. Thinking about your use of social networking or social media or gaming sites, have you seen any of these online?

(a) Report button (to tell someone if you are being treated badly online)

I don't know what it is	No, I haven't seen it	Yes. I have seen it	Yes, I know what it is and I have used it
1	2	3	4

(b) Help centre or link to a helpline (to contact someone who can help you)

I don't know what it is	No, I haven't seen it	Yes. I have seen it	Yes, I know what it is and I have used it
1	2	3	4

(c) Safety Centre (to get information or advice)

I don't know what it is	No, I haven't seen it	Yes. I have seen it	Yes, I know what it is and I have used it
1	2	3	4

65. For which of the following do you use Social media?

To share my life with friends	To get to know new friends	To get to know about others life	To get to know about fashion ,news etc.	Any other purpose
1	2	3	4	4

Thank you!

Annex 02



Research on the incidence, nature and scope of online violence against children, and the mechanisms that respond to cases of online violence against children Social Policy Analysis and Research Center (SPARC) University of Colombo

This is a questionnaire, to be self-administered by children aged 13-17 at home. This is part of the Research to end online violence against children in Sri Lanka. The questionnaire examines how children and young people engage with the internet and online or digital technologies in their everyday lives. It has been developed by Social Policy Analysis and Research Center (SPARC) based on work by EU Kids Online (EUKO).

























Question	Yes (1)	No (2)	Remarks
01. Have you EVER had contact on the internet with someone you have not met face-to-face before (excluding online purchases of goods/ of goods)? (Accepting requests, messaging – replying to strangers, sending and receiving pictures and videos, files and documents, links etc.)			
Number of individuals			Remarks
02. Number of individuals you have come in to contact in this manner?			
Male (1) Female (2)			Remarks
03. Gender			
Yes (1) No (2)			Remarks
04. In the PAST YEAR, have you EVER met anyone face-to-face that you first got to know through internet?			
Number of individuals			Remarks
05. Number of individuals you have come in to contact in this manner?			
Male (1) Female (2)			Remarks
06. Gender			
07. Purpose of the meeting			

Harm from online risk

08. In the PASTYEAR, has anything EVER happened online that bothered or upset you in some way (e.g., made you feel uncomfortable, scared or that you shouldn't have seen it)?

Scenario	Yes	No
1. Sending an indecent text messages		
2. Sending an indecent picture/clipart/video/text/script/audio clips/emails		
3. Sharing indecent picture/clipart/video/text/script/audio clips/emails		
4. Cyber Bullying (example: harassing or threatening or making abusive fun of someone using electronic means)		
5. Cyber Extortion		
6. Someone made sexual comments/indecent jokes about your body, appearance, a family member and those comments made you uncomfortable		
7. Someone shared an indecent image of you		
8. Someone sent you an indecent image that you did not ask for		
9. You received an unwanted advertisement/message that contained a link to an unwanted/indecent website		
10. You clicked on a link in a message sent you that showed indecent images of other people		
11. Identity theft (Someone hacked your profile/Someone created a fake profile using your details and images)		
12. Other (Pls Specify)		

09. In which online platform did you suffer the online violence?

							
Facebook	Instagram	twitter	imo	Viber	Watts app	Pinterest	Messenger
							
WeChat	Tik Tok	Google	Yahoo!	Gmail	Y MAIL	PUBG	Online games
							
Snap Chat	You Tube	Skype	Chrome	Mozilla	Windows Explorer	Safari	Face Time/ Duo

10. If 'yes' to any option given in question 9, answer the questions below. In the PAST YEAR, how often did the following happen?

Scenario	Just once or twice	At least every month	At least every week	Daily or almost daily	Prefer not to say
1. Receiving an indecent text messages					
2. Receiving an indecent picture/clipart/video/text/script/audio clips/emails					
3. Receiving indecent picture/clipart/video/text/script/audio clips/emails					
4. Cyber Bullying (example: harassing or threatening or making abusive fun of some one using electronic means)					
5. Cyber Extortion					
6. Someone made sexual comments/indecent jokes about your body, appearance, a family member and those comments made you uncomfortable					
7. Someone shared an indecent image of you					
8. Someone sent you an indecent image that you did not ask for					
9. You received an unwanted advertisement/message that contained a link to an unwanted/indecent website					
10. You clicked on a link in a message sent you that showed indecent images of other people					
11. Identity theft (Someone hacked your profile/Someone created a fake profile using your details and images)					
12. Other (Pls Specify)					

11.1 What was the most harmful online violence you experienced Please explain ?

.....
.....
.....
.....

11.2 When you were treated in this way online or via a mobile device, has it happened through any of the following?

By mobile phone calls	By messages sent to me on my phone	On a social networking site (e.g., Facebook, Twitter)	On a media sharing platform (YouTube, Instagram, Flickr etc.)	In a chat room	In an online game	Some other way	Prefer not to say
1	2	3	4	5	6	7	8

11.3 Why do you identify it to be the most harmful violence?

.....
.....
.....
.....

12. (a) Thinking now about the LAST TIME this happened to you, how upset were you about what happened?

Scenario	A little upset	Fairly upset	Very upset	Prefer not to say	Any other (Pls Specify)
1. Receiving an indecent text messages					
2. Receiving an indecent picture/clipart/video/text/script/audio clips/ emails					
3. Receiving indecent picture/clipart/video/text/script/audio clips/emails					
4. Cyber Bullying (example: harassing or threatening or making abusive fun of some one using electronic means)					
5. Cyber Extortion					
6. Someone made sexual comments/ indecent jokes about your body, appearance, a family member and those comments made you uncomfortable					
7. Someone shared an indecent image of you					
8. Someone sent you an indecent image that you did not ask for					
9. You received an unwanted advertisement/message that contained a link to an unwanted/indecent website					
10. You clicked on a link in a message sent you that showed indecent images of other people					
11. Identity theft (Someone hacked your profile/Someone created a fake profile using your details and images)					

(b) When this serious online violence took place , how long did you feel like that for?

I got over it straight away	I felt like that for a few days	I felt like that for a few weeks	I felt like that for a few months or more	I still feel the same	Prefer not to say
1	2	3	4	5	6

(c) Can you briefly describe any other impacts of that incident on you ?

13. (a) The last time something happened online that bothered or upset you, did you talk to anyone of these people about it?

My mother or father/ Guardians	Siblings	Cousins	A friend around my age	A friend who's older than my age	A teacher	Another adult I trust	I didn't talk to anyone	Prefer not to say
1	2	3	4	5	6	7	8	9

(b) When did you inform this individual about the incident?

On the very day it took place	The very next day	Few days after	A week after	After a month	Any other Pls Specify
1	2	3	4	5	6

(c) How did they respond to it?

Supported you in complaining to the authorities	Listened to you but did not take any action	Listened to you and advised you not to take any action	Listened briefly and Blamed you	Did not listen to you or take any action	Any other Pls Specify
1	2	3	4	5	6

(d) If you did not inform or refer to any of the above persons, why ?

I was scared	I was threatened With my life	I was threatened to reveal personal information	I was offered Gifts/money/ Goods to keep this as a secret	I was offered Gifts/money/ Goods to do this	I didn't want to lose that friendship/ relationship	He/she offered me emotional support	He/she was there for me when no one was there	Any other Pls Specify
1	2	3	4	5	6	7	8	9

14. (a) The last time something happened online that bothered or upset you, did you refer the incident to one of the following?

Police	Child Protection Officer	Child Rights Promotion Officer	Probation officers	1929 NCPA Help line	Government Counsellor	School Counsellor	I did NOT refer to any of these
1	2	3	4	5	6	7	8

(b) If you did NOT inform or refer to any of the above persons or institutions, why ?

I was scared	I was threatened With my life	I was threatened to reveal personal information	I was offered Gifts/money/ Goods to keep this as a secret	I was offered Gifts/money/ Goods to do this	I didn't want to lose that friendship/ relationship	He/she was there for me when no one was there	Any other Pls Specify
1	2	3	4	5	6	7	8

(c) If you informed any of those persons or institutions, can you briefly explain the actions taken by these organizations?

.....
.....
.....

(d) What is your feedback regarding the actions taken by the relevant persons or institutions ?

		Not Satisfied	Satisfied but should improve	Good / Extremely supportive	Other Remarks
		1	2	3	
(a)	Police				
(b)	Child Protection Officer				
(c)	Child Rights Promotion Officer				
(d)	Probation Officer				
(e)	1929 NCPA helpline				
(f)	Government Counsellor				
(g)	School Counsellor				

15. When this serious online violence took place, what was your immediate reaction ? (Multiple response question)

I ignored the problem or hoped the problem would go away by itself	I closed the window or app	I felt a bit guilty about what went wrong	I tried to get the other person to leave me alone	I tried to get back at the other person	I stopped using the internet/ app for a while	I deleted any messages from the other person	I changed my privacy/ contact settings	I reported the problem online (e.g., clicked on a 'report abuse' button, contacted an internet advisor or Internet Service Provider (ISP))	I followed the instructions of the person
1	2	3	4	5	6	7	8	9	10

16. If you selected option no 10 the above question, can you please explain why you selected it?

I was scared	I was threatened With my life	I was threatened to reveal personal information	I was offered Gifts/ money/ Goods to keep this as a secret	I was offered Gifts/ money/ Goods to do this	I didn't want to lose that friendship/ relationship	He/she offered me emotional support	He/she was there for me when no one was there	Any other Pls Specify
1	2	3	4	5	6	7	8	9

17. (a) It was never your fault that you became a victim of cyber violence. Do you think the way in which you used internet made you vulnerable to the perpetrator?

Yes	No
1	2

(b) If your answer is 'Yes' can you briefly explain what do you think that made you vulnerable to cyber violence ?

.....
.....
.....
.....
.....

(c) If you answer is 'No' can you briefly explain what factors might have made you vulnerable to cyber violence ?

.....
.....
.....
.....
.....

Thank you!

Annex 03

Child Safeguarding Risk Assessment Framework (CSRAF) Project:

Research on the incidence, nature and scope of online violence against children,
and the mechanisms that respond to cases of online violence against children
Social Policy Analysis and Research Center (SPARC)

University of Colombo

Activity	Identification of Abuse, Harm and other Risk situations	Analysis of Risk Factors
1. Conducting individualized interviews with (2400) number of children in (25) districts of age (13-17) And Conducting in-depth interviews with 50 children, selecting two from each district	<p>(a) Identification of the level and gravity of incidence of violence against children (VAC) and the resultant risk based on the criterion outlined in this CSRAF.</p> <p>The risk is categorised either as significant harm or less significant harm</p>	<p>Children may share information about the physical, psychological, emotional, and sexual abuses, harmful situations that may affect or/and endanger their physical, psychological & emotional security, safety and social wellbeing.</p> <p>Need to protect them from further harm should be recognized</p> <p>This requires referring the matters to relevant and appropriate child protection mechanisms or/and to law enforcement authorities.</p> <p>The level of risk/harm will be critical to determine the most appropriate mechanism to be referred to, based on this CSRAF</p> <p>Risk level of the child will be determined according to the following criterion, <i>significant harm & less significant harm</i></p> <p>Significant harm A child must have experienced at least one of the following forms of violence or similar type of violence or clear likelihood of an imminent threat to be subject to any or more of VAC should be identified as a significant harm. <i>Significant harm could a contact abuse or a non-contact abuse</i></p> <p>Contact abuse is where an abuser makes physical contact with a child, including penetration. It includes but not limited to:</p> <ul style="list-style-type: none"> • Sexual touching of any part of the body whether the child's wearing clothes or not • Rape or penetration by putting an object or body part inside a child's mouth, vagina or anus • Forcing or encouraging a child to take part in sexual activity • Making a child take their clothes off, touch someone else's genitals or masturbate. • Sexually exploiting a child for money, power or status (child exploitation).

Abbreviations:

COPINE	Combating Paedophile Information Networks in Europe
CSFP	Child Safeguarding Focal Point
CSRAF	Child Safeguarding Risk Assessment Framework
NA	Not Applicable
NGOs	Non-Governmental Organizations
NCPA	National Child Protection Authority
SCI	Save the Children International
SAP	Sentencing Advisory Panel
SPARC	Social Policy Analysis and Research Center
VAC	Violence Against Children

Risk	Mitigation Action to be taken	By Whom	By When	Budget	Action taken
H M L					
H	<p>When significant harm is present it requires to take immediate appropriate actions and referrals should be made to available services</p> <p><i>Available services” – includes services provided by the NCPA and DPCCS, hospital – based counselling services, National Mental Health Helpline – 1926, counselling and psychosocial support locally provided by NGOs such as LEADS, Shanthi Maargam etc</i></p>	<p>(a) Enumerators/research assistants are not expected to make any complaints to the authorities.</p> <p>(b) However, if they identify any form of abuse suffered by the child or disclosed by the child that shall be informed to the Research Team Leader and the Child Safeguarding Focal Point of the Research without delay.</p> <p>(c) Upon such an information is received following process can be followed:</p> <p>(i) The Child Safeguarding Focal Point (CSFP) of the Research and the Research Team Leader shall assess the risk level of the case by the application of CSRAF.</p> <p>(ii) If it is a significant harm the CSFP of the Research team shall share the details with the SCI Child Safeguarding Team as agreed by the Consortium.</p> <p>(iii) The action shall be decided together by both the CSFP of Research and the SCI on a case by case system.</p> <p>(b) If there’s an immediate danger to the life of the child, if it is deemed that there is limited time, the CSFP of the Research shall inform through the hotline of the NCPA (1929).</p>	During filed work	N/A	

Activity	Identification of Abuse, Harm and other Risk situations	Analysis of Risk Factors	
		<p>A. Non-contact abuse is where an abuser does not make physical contact with the child, such as grooming, persuading children to perform sexual acts over the internet and flashing, including but not limited to:</p> <ul style="list-style-type: none"> • Encouraging a child to watch or hear sexual acts • Not taking proper measures to prevent a child being exposed to sexual activities by others • Meeting a child following sexual grooming with the intent of abusing them • Online abuse including making, viewing or distributing child abuse images • Allowing someone else to make, view or distribute child abuse images • Showing pornography to a child <p>* According to COPINE Scale, SAP Scale and 2014 UK Sexual Offences Definitive Guidelines, (*Refer to the Appendices)</p> <ul style="list-style-type: none"> • Images involving penetrative sexual activity • Images involving sexual activity with an animal or • Sadism <p>fall into significant harm category</p>	
		<p>Less Significant harm</p> <p>A child must have experienced at least one of the following criterion or similar type of experience or a reasonable fear of being subjected to any or more of those violence to be identified as less significant harm</p> <ul style="list-style-type: none"> • Isolated incidents of corporal punishment that do not leave a physical mark on the child • Isolated incidents of Emotional/ Mental violence 	

	Risk H M L	Mitigation Action to be taken	By Whom	By When	Budget	Action taken
			(a) Enumerators/research assistants are not expected to make any complaints to the authorities regarding less significant harm too. (b) However, if they identify any form of abuse suffered by the child or disclosed by the child that shall be informed to the Research Team Leader and the Child Safeguarding Focal Point of the Research without delay. (c) Upon such an information is received following process can be followed: (i) The Child Safeguarding Focal Point (CSFP) of the Research and the Research Team Leader shall assess the risk level of the case by the application of CSRAF. (ii) The action shall be decided together by both the CSFP of Research and the SCI on a case by case system.	During filed work	N/A	

Activity	Identification of Abuse, Harm and other Risk situations	Analysis of Risk Factors	
	(b) Assess the potential of sharing and revealing of sensitive information to cause agitation or distress to children themselves or/and to their parents or guardians.	Sharing sensitive information may expose them to social stigma and cultural isolations.	
2. Conduct focus group discussions (FGDs) with 10 children in each District (age group 13-17)	Information on incidences of online VAC should be identified and dealt with the application of CSRAF. The criterion of significant harm and less significant harm mentioned in CSRAF should be the rational in identifying the risk and vulnerability levels		
3. Interviews with 20 KIIs (Experts in the field of child protection and law enforcement)	KIIs may expose incidents of online VAC to the research team and sensitive information that they possess	If sensitive information and personalized information will be disclosed to the research team the exposition of such information with the identifying details would harm the right to privacy of children if such details would be publicized.	

Appendices:

- A. The COPINE Scale
- B. The SAP Scale
- C. The Sexual Offences Definitive Guideline 2014 – UK

Risk			Mitigation Action to be taken	By Whom	By When	Budget	Action taken
H	M	L					
	M		This may require referring the matter to non-legal referral services.	The Child Safeguarding Focal Point (CSFP) of the Research and the Research Team Leader shall assess the vulnerability level of such cases by the application of CSRAF. (ii) The action shall be decided together by both the CSFP of Research and the SCI on a case by case system.	During filed work		
			If the information, received at the FGDs, would disclose evidence about significant harm such matters should be referred to “Appropriate Authorities” as outlined in the other column. If the matter is assessed as more appropriate to refer to other authorities such as District/Divisional level NCPA officers, DPCCS officers or CRPOs the information on how to access such places should be given.	When such information is received following process should be followed: (i) The Child Safeguarding Focal Point (CSFP) of the Research and the Research Team Leader shall assess the risk levels of the case by the application of CSRAF. (ii) If it is a significant harm the CSFP of the Research team shall share the details with the SCI Child Safeguarding Team as agreed by the Consortium. (iii) The action shall be decided together by both the CSFP of Research and the SCI on a case by case system. (b) If there’s an immediate danger to the life of the child, if it is deemed that there is limited time, the CSFP of the Research shall inform through the hotline of the NCPA (1929),	During filed work	N/A	
			Prior to the KII interviews to be conducted, KIIs should be instructed to keep the confidential, sensitive and personalized information as matters not to be disclosed in public and to the media	Research team should maintain the confidentiality of such information and research ethics should be duly observed.	During KIIs	N/A	

A. The COPINE Scale

The COPINE Scale	
1. Indicative	Non-erotic and non-sexualised pictures showing children in their underwear, swimming costumes from either commercial sources or family albums. Pictures of children playing in normal settings, in which the context or organisation of pictures by the collector indicates inappropriateness.
2. Nudist	Pictures of naked or semi-naked children in appropriate nudist settings, and from legitimate sources.
3. Ero	Surreptitiously taken photographs of children in play areas or other safe environments showing either underwear or varying degrees of nakedness.
4. Posing	Deliberately posed pictures of children fully clothed, partially clothed or naked (where the amount, context and organisation suggests sexual interest).
5. Erotic Posing	Deliberately posed pictures of fully, partially clothed or naked children in sexualised or provocative poses.
6. Explicit Erotic Posing	Pictures emphasising genital areas, where the child is either naked, partially clothed or fully clothed.
7. Explicit Sexual Activity	Pictures that depict touching, mutual and self-masturbation, oral sex and intercourse by a child, not involving an adult.
8. Assault	Pictures of children being subject to a sexual assault, involving digital touching, involving an adult.
9. Gross Assault	Grossly obscene pictures of sexual assault, involving penetrative sex, masturbation or oral sex, involving an adult.
10. Sadistic/ Bestiality	a. Pictures showing a child being tied, bound, beaten, whipped or otherwise subject to something that implies pain.

B. The SAP scale

The SAP Scale	
1.	Nudity or erotic posing with no sexual activity
2.	Sexual activity between children, or solo masturbation by a child
3.	Non-penetrative sexual activity between adult(s) and child(ren)
4.	Penetrative sexual activity between child(ren) and adult(s)
5.	Sadism or bestiality

C. Sexual Offences Definitive Guideline 2014 - UK

Category A

Images involving penetrative sexual activity and/or images involving sexual activity with an animal or sadism

Category B

Images involving non-penetrative sexual activity

Category C

Other indecent images not falling within categories A or B

Consortium to End Online Violence Against Children, Sri Lanka

The Consortium to End Online Violence Against Children in Sri Lanka was formed in 2018 under the aegis of the Ministry of Women and Child Affairs and Dry Zone Development (predecessor of the State Ministry of Women and Child Development, Pre-Schools & Primary Education, School Infrastructure & Education Services) with Save the Children, Sri Lanka as its leading partner and World Vision Lanka and LEADS as its co-partners. Through this Consortium, the Partner Organizations implemented the Project – End Online Violence Against Children in Sri Lanka with the support provided by the Global Partnership to End Violence Against Children (GPEVAC).



State Ministry of Women and Child
Development, Pre-School & Primary
Education, School Infrastructure &
Education Services



Save the Children



ISBN: 978-624-5738-01-4