UNODC
United Nations Office on Drugs and Crime

Study on the **Effects of New Information Technologies** on the Abuse and Exploitation of Children

UNITED NATIONS OFFICE ON DRUGS AND CRIME
Vienna

Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children

UNITED NATIONS
New York, 2015

Publishing production: English, Publishing and Library Section, United Nations Office at Vienna.

Acknowledgements

This report was prepared pursuant to ECOSOC resolution 2011/33 on Prevention, protection and international cooperation against the use of new information technologies to abuse and/or exploit children by Conference Support Section, Organized Crime Branch, Division for Treaty Affairs, UNODC, under the supervision of John Sandage (former Director, Division for Treaty Affairs), Sara Greenblatt and Loide Lungameni (former and current Chief, Organized Crime Branch, respectively), and Gillian Murray (former Chief, Conference Support Section).

Study team:

Steven Malby, Tejal Jesrani, Tania Bañuelos, Anika Holterhof, Magdalena Hahn (UNODC).

Consultant:

Kayla Bakshi

Experts:

The study greatly benefited from the inputs of the following expert practitioners in the fields of law enforcement, prosecution, academia, the private sector and civil society:

Maria Teresa Aguirre, Paraguay
Anjan Bose, ECPAT International
John Carr, Online Child Safety Consultant
Carla Della Donne, Argentina
Guillermo Gallarza, International Center for Missing and Exploited Children
Paul Gillespie, Kids' Internet Safety Alliance (KINSA)
Jorge Luis San Lucas Gonzalez, Ecuador
Susie Hargreaves, Internet Watch Foundation
Apichart Hattasin, Thailand
Jenny Jones, GSMA
Lata Kallychurn, Mauritius
Carla Licciardello, International Telecommunications Union (ITU)
Bjørn-Erik Ludvigsen, Norway
Nelly Montealegre, Mexico
Michael Moran, INTERPOL
Andrew Morling, United Kingdom
Omashani Naidoo, South Africa
Heila Niemand, South Africa
John Peacock, New Zealand
John Penn, Adobe
Cristian Perella, Facebook
Anders Persson, Sweden
Ethel Quayle, COPINE Project
Patrick Redling, Virtual Global Task Force
Jonathan Rouse, Australia
Seila Samleang, APLE Cambodia
Vanessa Fusco Simoes, Brazil
Hana Snajdrova, Organization for Security and Co-operation in Europe (OSCE)
Clara Sommarin, United Nations Children's Fund (UNICEF)
Oran Sukkasem, Thailand
Joe Sullivan, Mentor Forensic Services
Daniel Szumilas, Germany
Janis Wolak, Crimes against Children Research Center

The Branch is also grateful for the input of UNODC staff members Margaret Akullo, Adam Palmer, Anna Giudice Saget and Alexandra Souza Martins.

Contents

List of abbreviations

CCPCJ	Commission on Crime Prevention and Criminal Justice
CEOP	Child Exploitation and Online Protection Centre
CEPT	Confederation of European Posts and Telecommunications
CETS	Child Exploitation Tracking System
CIRCAMP	COSPOL Internet Related Child Abusive Material Project
COSPOL	Comprehensive, Operational, Strategic Planning for the Police
CRC	Convention on the Rights of the Child
EFC	European Financial Coalition
EU	European Union
GPS	Global Positioning System
GSMA	Groupe Speciale Mobile Association
HTML	Hyper-Text Markup Language
ICMEC	International Center for Missing and Exploited Children
ICT	Information and communication technology
ILO	International Labour Organization
INHOPE	International Association of Internet Hotlines
INTERPOL	International Criminal Police Organisation
IP	Internet Protocol
ISP	Internet service provider
ITU	International Telecommunications Union
IWF	Internet Watch Foundation
IWOL	INTERPOL "worst of" list
NCMEC	National Center for Missing and Exploited Children
NGO	Non-governmental organization
OECD	Organisation for Economic Co-operation and Development
OPSC	Optional Protocol to the Convention on the Rights of the child on the sale of children, child prostitution and child pornography
OCSARP	Online Child Sexual Abuse Reporting Portal
SIM	Subscriber identification module
SMS	Short Message System
UNHCR	United Nations High Commissioner for Refugees
UNICEF	United Nations Children's Fund
UNODC	United Nations Office on Drugs and Crime
UNTOC	United Nations Convention against Transnational Organized Crime
URL	Uniform resource locator
VGT	Virtual Global Taskforce
WHO	World Health Organization

Executive summary

This Study on the effects of new information technologies on the abuse and exploitation of children was prepared pursuant to Economic and Social Council resolution 2011/33 on Prevention, protection and international cooperation against the use of new information technologies to abuse and/or exploit children, in which the Council expressed concern that increasingly rapid technological advances have created new possibilities for the criminal misuse of new information and communication technologies.

The study is based primarily on open source research and the outcomes of an informal expert group meeting on ICT-facilitated abuse and exploitation of children, held in Vienna from 23 to 25 September 2013. In accordance with Council resolution 2011/33, relevant information from the 2013 Comprehensive Study on Cybercrime prepared for the consideration of the open-ended intergovernmental expert group on cybercrime is also taken into account. The study is divided into four chapters and contains a glossary as an annex.

Introduction

Fast-paced technological innovation and widespread and increasing accessibility of ICTs, including high-speed Internet and mobile devices with Internet connectivity, have transformed societies around the world. Children in particular have increased access to ICTs and, in recent decades, have tended to adopt these technologies from an early age, resulting in ICTs becoming thoroughly embedded in their lives.

This context facilitates opportunities for the misuse of ICTs to abuse and exploit children. Children can easily engage with strangers and exchange large data files, while the possibilities for parental supervision and monitoring are restricted. Children are also at particular risk as they often do not fully understand threats associated with the use of ICTs, or are not sufficiently aware that, once shared, control over such material is effectively waived.

Advances in ICTs can also facilitate criminal collaboration and communication, while law enforcement agencies may frequently lack the human and financial resources, technical capacity and appropriate legal tools to investigate digital crime. Cultural variations and differences in legal systems can also further complicate effective prevention and investigations.

Efforts to effectively and comprehensively combat ICT-facilitated child abuse and exploitation necessitate a multi-stakeholder approach, including and actively involving children, families, communities, governments, members of civil society and the private sector.

I. Identifying and describing the problem

Differences in the definition of "child" under national legal systems may lead to varying responses to child abuse and exploitation. While the term "abuse" focuses more on the treatment of the child victim, "exploitation" refers more to the benefit of the offender.

"Contact" and "non-contact" sexual abuse are distinguished from one another in terms of physical conduct involving children. Contact sexual abuse generically refers to in-person sexual contact of a harmful nature, while non-contact sexual abuse denotes acts where the perpetrator does not come into physical contact with a child, such as in the case of possession, distribution or consumption of child sexual abuse material.

"Commercial sexual exploitation of children" refers to the exploitation by an adult of a child, accompanied by payment in money or in kind to the child or to one or more third parties. It encompasses an array of commercial offences, including the prostitution of children, arrangement of child marriage, and child sex tourism. Non-commercial exploitation pertains to exploitative acts committed for personal gratification rather than for financial or economic gain. Personal gratification may nevertheless coincide with obtaining economic benefit, such as when a trafficker abuses children he or she intends to exploit.

The main forms of ICT-facilitated child abuse and exploitation can be identified by observing practices. The forms discussed in this study are: child sexual abuse material (child pornography); commercial sexual exploitation of children; cyberenticement, solicitation and grooming; cyberbullying, cyberharassment and cyberstalking; and exposure to harmful content.

"Child sexual abuse material" comes in many forms and consists of a recording, usually in still or video, which depicts a child engaged in sexually explicit activity.

The terms "cyberenticement", "solicitation" and "online grooming" are regularly used collectively or interchangeably to

describe communications made by adults through the use of ICTs for the purpose of sexually abusing or exploiting minors.

"Cyberharassment" refers to the intimidation, repeated or otherwise, of one individual by another or by a group, perpetrated through or utilizing electronic means.

"Cyberbullying" encompasses the use of ICTs to harm a victim or victims in deliberate, repeated, and hostile ways. "Cyberstalking" is commonly understood as a course of action that involves more than one incident perpetrated through or utilizing electronic means that causes distress, fear or alarm.

"Exposure to harmful online content" pertains to situations where a child accidentally or intentionally views pornographic or other content that is judged to be harmful to their development, sexual or otherwise.

II. Evaluating the problem

Effects of information and communication technologies on common forms of child abuse and exploitation

Potential offenders are able to gain enhanced access to victims and to child sexual abuse material through the use of ICTs, which increase their pool of potential victims, offer the opportunity of creating false identities, and facilitate the transmission of harmful content to children. Human traffickers may also recruit new victims, including children, and market child sex tourism through the use of ICTs.

ICTs can deliver increased profits for criminal enterprises by markedly reducing the costs of production and distribution of child sexual abuse material. Human traffickers may also carry out their activities primarily, or even exclusively, via mobile phone. The use of mobile phones and the Internet further assists offenders in hiding their identities and obfuscating activities, thus reducing risk of detection.

Increased levels of harm and re-victimization can occur through "layering" of crimes such as, for instance, when child sexual abuse material is produced, and then distributed and redistributed online. In addition, cyberbullies may use public websites and social media to broaden their audience and increase the impact on victims.

Ever-increasing levels of violence coupled with the continuously decreasing age of victims in child sexual abuse material have been observed. Increasingly large amounts of readily available online child sexual abuse material also serve to desensitize viewers, resulting in a demand for ever more extreme material.

The use of ICTs affords unprecedented provision of social affirmation for offenders. Readily available child sexual abuse material online may create the false impression of social acceptability. Online communities can also provide forums for sharing strategies to gain access to victims and to evade law enforcement.

New forms of child abuse and exploitation

Made-to-order child sexual abuse material can be linked with organized criminal group activities and is a significant and emerging threat. The increasing demand for new images appears to be reflected in escalating prices for such material.

In the context of child abuse and exploitation, self-generated content comprises images and videos that are produced by and feature children. This includes conduct such as "sexting", a form of self-generated sexually explicit content. Mass availability of ICTs has increased the production of and loss of control over self-generated content.

As Internet access proliferates and becomes increasingly affordable, perpetrators can broadcast live sex abuse of children. Live images of abuse may also be recorded for future distribution in order to generate maximum profit.

Victimization risk factors

Girls account for the majority of victims of child abuse and exploitation, although boys are increasingly at risk as well. Prior abuse and family dysfunction may elevate the risk of victimization, particularly for commercial sexual exploitation of children. Poverty and migration and social isolation can also have negative repercussions on patterns of commercial sexual exploitation of children.

Very young children are increasingly victimized in child sexual abuse material and child sex trafficking and exploitation. Adolescents face the highest risk of cyberenticement, exposure to harmful material and cyberbullying.

Children who engage in risky online behaviour and inattention to online safety and privacy face a higher risk of exploitation, cyberenticement, solicitation or grooming.

Profile of offenders

The motivations of offenders for committing child sex abuse vary. Many possessors of child sexual abuse material are preferential child sex offenders, or paedophiles. Preferential sex offence conduct is also linked to the commercial sexual abuse

and exploitation of children in the travel and tourism industries.

Both men and women participate in child exploitation, although males constitute the majority of perpetrators in child abuse. Male child sexual abuse material-users and producers are, most commonly, adults in the range of 25 to 40 years of age.

Both men and women may engage in cyberstalking and gender does not constitute a prominent feature in the profile of cyberbullies. Cyberbullying is especially prominent amongst children aged approximately 10 to 13 years. Though less common, some adults may also engage in cyberbullying of children.

Child sexual abuse material offenders can have comparatively high levels of education, and this may correlate to offenders' comfort with and sophistication in the use of technology. Both online and offline abusers may be more likely to have themselves experienced physical and sexual abuse than the general population.

Groups of perpetrators constituting organized criminal groups are active in the area of online child abuse, most commonly through the production and distribution of child sexual abuse material and commercial sexual exploitation of children. The structure of such groups can consist of Internet-based social networks of actors who collaborate in both commercial and non-commercial online trading of child sexual abuse material.

III. Combating the problem

International law increasingly recognizes that children deserve special protection. A number of international legal instruments require that States take measures to protect children from abuse and exploitation, as well as to engage in international cooperation in the investigation and prosecution of child abuse and exploitation crimes.

States vary considerably in approaches to addressing forms of child abuse and exploitation. While many States criminalize acts such as production of child sexual abuse material, they may differ with respect to elements of the crime and definitions of "child". Some countries have enacted laws that are specific to the commission of child exploitation offences using ICTs, while other States rely on general criminal laws against abuse and exploitation.

In some countries, there may be little or no legal basis for police to take action against child abusers and exploiters if the victim has already reached the legal age of consent, even though the child is still under 18 years of age. Most jurisdictions set the age of consent for sexual activity below 18 years of age, with the average ranging from 13 to 16 years.

Tools and mechanisms for international cooperation include mutual legal assistance treaties, direct law enforcement cooperation, multi-agency partnerships, forums for information-sharing and informal direct law enforcement cooperation. Significant challenges nevertheless still exist in achieving effective international cooperation regarding online investigations and electronic evidence in criminal matters.

Specific tools can be employed for detection and investigation, such as the use of digital forensic techniques, automated search, image analysis and image databases, data mining and analytics.

The private sector is also a key actor in the prevention of such crimes. Electronic service providers may engage in this respect through varying degrees of self-regulation, including by Internet service providers, self-monitoring by travel and tourism companies and the creation of financial coalitions.

Parents, guardians, child educators and civil society are a further vital component in combating the problem, including in supporting children in understanding and handling online risks, the "flagging" of certain material online, the creation of telephone hotlines for reporting, and contributions towards education and psycho-social methods of prevention.

Opportunities to enhance the fight against ICT-facilitated child abuse and exploitation

In enhancing the fight against ICT-facilitated child abuse and exploitation, governments and national authorities may focus on a child protection approach that fully respects human rights; on ensuring that legislation keeps pace with technological innovation; on recruiting, training and maintaining specialized personnel; on gaining access to state-of-the-art technological resources; developing effective mechanisms for accessing third party data and conducting undercover investigations that are consistent with the rule of law; as well as developing policy-guidance on harmful conduct committed by youth. The formulation of policies in this area is best based on a multidisciplinary approach that draws on research findings and best practices from social science, legal policy and public policy.

INTRODUCTION

This study was prepared pursuant to Economic and Social Council resolution 2011/33 on Prevention, protection and international cooperation against the use of new information technologies to abuse and/or exploit children, in which the Council expressed concern that increasingly rapid technological advances have created new possibilities for the criminal misuse of new information and communication technologies. In the same resolution, the Council requested the United Nations Office on Drugs and Crime (UNODC) to carry out a study facilitating the identification, description and evaluation of the effects of new information technologies on the abuse and exploitation of children, while taking into account relevant studies carried out by regional organizations and other organizations within the United Nations system, such as the United Nations Children's Fund, the International Telecommunication Union and the Office of the United Nations High Commissioner for Human Rights, with a view to promoting the exchange of experience and good practices.

Several factors have given rise to growing concerns over the effects of new information and communications technologies (ICTs) on the abuse and exploitation of children. In recent decades, technological innovation has profoundly transformed societies around the world. By the end of 2013, almost 40 per cent of the world's population, i.e. 2.7 billion people, and 78 per cent of households in developed countries had access to the Internet.[1] Although only 28 per cent of households currently have access to the Internet in developing countries, between 2009 and 2013 there were annual Internet access growth rates of 27 per cent in Africa and 15 per cent in Asia and the Pacific, the Arab States and the Commonwealth of Independent States.[2]

In developed countries, the rate of mobile-cellular penetration reached 128 per cent in 2013, indicating that some users have multiple sources of mobile-cellular access.[3] In the developing world, mobile cellular penetration rates reached 89 per cent at the end of 2013, marking a 20 per cent increase from 2010.[4] Along with the rising use of mobile phones, texting by Short Message System (SMS) has emerged as a common means of communication. Between 2007 and 2010, the number of SMS sent globally tripled from 1.8 trillion to 6.1 trillion a year, equaling an average of 200,000 text messages sent every second.[5] High-speed Internet has also spread significantly in recent years, greatly enhancing users' ability to exchange image and video files. By the end of 2010, 24 per cent of the developed world had adopted fixed broadband Internet access.[6] Although in the developing world only 6 per cent of households have adopted fixed broadband, many developing countries are increasingly embracing mobile broadband technology with the advent of smartphones, tablets and other wireless devices.[7]

The result of these trends is a global population, and in particular a global youth, with ever ready access to ICTs. In general, global data indicates that children's Internet usage is increasing, both with regard to the number of children going online and time spent on the Internet.[8] In recent decades children have tended to adopt ICTs from an early age, such that ICT becomes thoroughly embedded in their lives.[9] For instance, 25 per cent of children in the United States under the age of six are online regularly, and nearly 60 per cent of children between the ages of six and nine years use the

[1] Child Exploitation and Online Protection Centre (CEOP), 2013. *Threat Assessment of Child Exploitation and Sexual Exploitation and Abuse*. Paragraph 17.

[2] International Telecommunications Union (ITU), 2014. *The World in 2013: Facts and Figures*.

[3] *Ibid.*

[4] ITU, 2011. *The World in 2010: Facts and Figures*.

[5] *Ibid.*

[6] *Ibid.*

[7] ITU, 2014.

[8] UNICEF, 2011. *Child Safety Online. Global challenges and strategies.* Pp. 3-4.

[9] ITU, 2008. *Use of Information and Communication Technology by the World's Children and Youth*; see also UNICEF, 2011. P. v; Michelet, I., 2003. *Our Children at Risk Online. The Example of Thailand. A Survey Report.* P. 12. Available at: http://www.ecpat.net/sites/default/files/Our_Children_At_Risk_Online_ENG.pdf.

Internet every day.[10] Similarly, in 2011, the Internet usage rate of children aged 3 to 5 in South Korea was at 66 per cent.[11] In Europe, 9 to 16-year-olds use the Internet for between one and five hours per day, while in Bahrain, the average daily time of Internet use ranges between two and a half and three and a half hours per day. Nonetheless, disparities in Internet access remain. Recent data shows, for example, that South African minors access the Internet more infrequently and for comparatively shorter periods of time than in developed countries.[12] Bridging the still-existing digital divide between the developed and developing world by promoting free and equitable access to the Internet is a policy priority for the United Nations and its Member States.[13]

In addition to bringing social, educational, economic and cultural benefits, however, the expansion of availability and accessibility of ICTs has also created a number of threats to the safety of individuals and especially of children, who are particularly vulnerable to ICT-facilitated abuse and exploitation.[14]

The ongoing proliferation of broadband Internet access and mobile phones plays a pivotal role in facilitating online child abuse as mobile devices greatly widen the range of contacts, including strangers or Internet-only contacts, that children encounter, in an environment where possibilities for parental supervision and monitoring of activities can be significantly restricted.[15] Once online, children and adolescents engage in a broad spectrum of activities in areas ranging from gaming and entertainment to education and social interaction. In particular, social networking, which enables users to post and exchange personal information, photos and videos, build networks of friends, and maintain high levels of interaction and information exchange on every aspect of daily life, is prevalent among young Internet users. Data from 2011 indicate that 73 per cent of teenagers in the United States, and 59 per cent of 9 to 16-year-olds in the European Union had a social networking profile, while an estimated 12 per cent of the 37 million Indian, and approximately 13 per cent of the 29 million Brazilian Facebook-users were between 13 and 17 years of age.[16]

While increased and more frequent usage of ICTs entails a heightened risk of infringements on privacy and safety for all users, children are at particular risk, as they often do not fully understand the threats associated with these technologies, especially when it comes to sharing of personal information, photos or videos.[17] A 2008 study in the United States showed, for instance, that one in five American adolescents between the ages of 13 and 19 had sent or posted nude or semi-nude pictures of themselves online.[18] Young people frequently do not understand or are not sufficiently aware that they effectively waive control over such images once shared.[19]

The problem is aggravated by the fact that parents and other caregivers often struggle with a lack of technological sophistication, making it difficult for them to make use of existing safety and privacy tools to protect their children and supervise their online activities. Even where parents have adequate technological knowledge, portable devices present a particular challenge to successful supervision and protection. Research in Europe, for example, has found that 49 per cent of children access the Internet from their bedrooms and 33 per cent use mobile devices.[20] A recent threat assessment concerning child exploitation and sexual exploitation and abuse conducted by the United Kingdom Child Exploitation and Online Protection Centre (CEOP) concluded that "direct parental supervision of children's Internet use is increasingly unfeasible."[21]

Advances in ICTs also facilitate criminal collaboration and communication across jurisdictions and borders with regard to the commission of acts of child abuse and exploitation. Law enforcement agencies often lack the human and financial resources, as well as technical capacity and appropriate tools to thoroughly and effectively investigate such transnational crimes. Whereas criminals can quickly invent, implement

[10] Gutnick A., et al., 2011. *Always Connected: The New Digital Media Habits of Young Children*. Pp. 14-18. Available at http://www.joanganzcooneycenter.org/wp-content/uploads/2011/03/jgcc_alwaysconnected.pdf.

[11] http://www.statista.com/statistics/226730/Internet-usage-of-young-children-in-south-korea-since-2006/.

[12] UNICEF, 2011. Pp. 3-4; see also Michelet, I., 2003. P. 13.

[13] Ruggie, J., Dossal, A., 2000. *Towards Bridging the Digital Divide. A Discussion Paper.*

[14] UNICEF, 2011. P. 3.

[15] UNICEF, 2011. P. 4.

[16] See e.g. UNICEF, 2011. P. 4.

[17] See e.g. UNICEF, 2011. P. 5.

[18] National Campaign to Prevent Teen and Un-planned Pregnancy, 2008. *Sex and Tech: Results of a Survey of Teens and Young Adults*. Available at: www.thenationalcampaign.org/SEXTECH/PDF/SexTech_Summary.pdf; see also UNICEF, 2011. P. 5.

[19] Quayle, E., 2013. *Commentary at the Informal Expert Group Meeting on the Effects of Information and Communication Technologies on the Abuse and Exploitation of Children.* Vienna. September 23, 2013 through September 26, 2013.

[20] Livingstone, S., Haddon, L., Görzig A., Ólafsson, K., 2011. *EU Kids II.* P. 2; see also CEOP, 2013. Paragraph 52.

[21] CEOP, 2013. Paragraph 52; see also UNICEF, 2011. Pp. 7-8.

and adapt to the commission of technology-facilitated crime, policymakers and investigators must undergo the process of researching the issues, forging consensus and developing legal and investigative responses in order to address newly emerging forms of ICT-facilitated crime. In the international context, cultural variations and differences in legal systems and traditions can further complicate the work of and cooperation between law- and policymakers as well as law enforcement agencies. In addition, the fact that a significant proportion of Internet infrastructure is owned and operated by the private sector, requires the close engagement of private sector service providers. Efforts to effectively and comprehensively combat ICT-facilitated child abuse and exploitation thus necessitate a multistakeholder approach, including and actively involving children, families, communities, governments, members of civil society and the private sector.[22]

It is important to note that not all forms of ICT-facilitated child abuse and exploitation fundamentally diverge from those that are not facilitated by ICTs. In fact, many forms of ICT-facilitated child abuse and exploitation involve the same dynamics, patterns and structures as non-digital ones[23] and in many cases, ICTs only serve to facilitate the commission of already-known types of crimes and forms of criminality. On the other hand, new information technologies have also given rise to some new forms of child abuse and exploitation that are enabled exclusively through the use of ICTs. This study seeks to identify and describe some of the more common forms of ICT-facilitated child abuse and exploitation, with a view to a complete picture of the problem and the formulation of a comprehensive approach to prevent and combat such crimes.

Scope and structure of the study

The preparation of the study was facilitated by an informal expert group meeting on ICT-facilitated abuse and exploitation of children, held in Vienna from 23 to 25 September 2013. The meeting brought together international experts from law enforcement, research, industry and civil society.

This study is based primarily on open source research and the outcomes of the informal expert group meeting. In accordance with the mandate of ECOSOC resolution 2011/33, it also takes into account documents and materials from other entities of the United Nations system. Where relevant, it makes reference to information from the 2013 Comprehensive Study on Cybercrime prepared by UNODC for the consideration of the open-ended intergovernmental expert group on cybercrime (hereinafter, "Cybercrime Study").[24] The Cybercrime Study was based on information received by UNODC from 69 Member States, 40 private sector organizations, 16 academic organizations and 11 intergovernmental organizations, and included a review of more than 500 open source documents obtained through systematic academic and enterprise literature searches.

Of particularly relevance to the present study is the description contained in the Cybercrime Study of the various acts and courses of conduct constituting cybercrime in general. This is reproduced in figure I below. The list includes 14 distinct types of acts falling into three broader categories of cybercrime, as indicated in the table below.[25]As noted in the Cybercrime Study, the list is not intended to be exhaustive, but rather to represent "act descriptions" that can be used as a starting point for analysis and discussion.

[22] UNICEF, 2011. P. vi.

[23] UNICEF, 2011. P. vi.

[24] In its resolution 65/230, the General Assembly requested the Commission on Crime Prevention and Criminal Justice (CCPCJ) to establish, in line with paragraph 42 of the Salvador Declaration on Comprehensive Strategies for Global Challenges: Crime Prevention and Criminal Justice Systems and Their Development in a Changing World, an open-ended intergovernmental expert group, to conduct a comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector, including the exchange of information on national legislation, best practices, technical assistance and international cooperation, with a view to examining options to strengthen existing and to propose new national and international legal or other responses to cybercrime. In its resolution 67/189, the General Assembly noted with appreciation the work of the open-ended intergovernmental expert group to conduct a comprehensive study of the problem of cybercrime and encouraged it to enhance its efforts to complete its work and to present the outcome of the study to the Commission on Crime Prevention and Criminal Justice in due course. The first session of the expert group was held in Vienna from 17 to 21 January 2011. At that meeting, the expert group reviewed and adopted a collection of topics and a methodology for the study. At its second meeting, held from 25 to 28 February 2013, the expert group considered the draft comprehensive study prepared by the Secretariat on behalf of the group, as tasked by the methodology agreed by the expert group at its first session in 2011, on the basis of information received from Member States, intergovernmental organizations, enterprises, and academia. During its 22nd session, the CCPCJ expressed its appreciation for the work done thus far by the expert group and in Resolution 22/7 requested the group to continue its work towards fulfilling its mandate.

[25] UNODC, 2013. *Cybercrime Study*. P. 16.

Figure I. Cybercrime act descriptions

Acts against the confidentiality, integrity and availability of computer data or systems

- Illegal access to a computer system
- Illegal access, interception or acquisition of computer data
- Illegal interference with a computer system or computer data
- Production, distribution or possession of computer misuse tools
- Breach of privacy or data protection measures

Computer-related acts for personal or financial gain or harm

- Computer-related fraud or forgery
- Computer-related identity offences
- Computer-related copyright or trademark offences
- Sending or controlling the sending of Spam
- Computer-related acts causing personal harm
- Computer-related solicitation of "grooming" of children

Computer content-related acts

- Computer-related acts involving hate speech
- Computer-related production, distribution or possession of child pornography
- Computer-related acts in support of terrorism offences

Source: Comprehensive Study on Cybercrime, 2013.

Three of these act descriptions have particular relevance for the consideration of child abuse and exploitation: computer-related acts causing personal harm; computer-related solicitation or "grooming" of children; and computer-related production, distribution and possession of child pornography. These acts are by no means exhaustive of the type of offences for which children may fall victim through ICT, but they do provide a good starting point for discussion. The first two acts fall into the category of "computer-related acts for personal or financial gain or harm" and the third under "computer content-related acts".

"Computer-related acts for personal or financial gain or harm" refer to "acts for which the use of a computer system is inherent to the *modus operandi*" and in which the object of the offence may be regarded as the individual targeted, such as through the use of a computer system to harass, bully, threaten, stalk or to cause fear or intimidation of an individual, or "grooming" of a child. As noted in the Cybercrime Study, one challenge is that this category may include a broad range of otherwise offline crimes, when committed with the use or help of a computer system.[26] The category of "computer content-related acts" concerns computer content—the words, images, sounds and representations transmitted or stored by computer systems, including the Internet. The material offence object in content-related offences is often a person, an identifiable group of persons, or a widely held value or belief. Similar to the category of computer-related acts for personal or financial gain or harm, these acts could, in principle, be committed offline, as well as through the use of computer systems.[27] Within both broad categories of acts, clear legislation and definitions are key for providing well-defined criminalization of conduct especially related to ICT-facilitated child abuse and exploitation. In particular, some courses of conduct may cut across categories, such as when a child is both "groomed" online and persuaded to send personal images of a sexual nature.

The remainder of the study is divided into four parts. Chapter I builds on the above by identifying and defining key terms in analysing the problem of ICT-facilitated child abuse and exploitation. It describes the most common types and forms of related behaviour, utilizing terminology that seeks to provide an effective description of relevant phenomena, practices and acts, which may or may not be currently criminalized in all jurisdictions. Chapter II evaluates the effects of ICTs on common and new forms of child abuse and exploitation, and describes how the use of information and communication technologies in the commission of offences can increase the levels of harm to victims. Chapter II also provides a brief overview of the main risk factors for victims as well as potential offender profiles. It briefly describes organized groups of offenders and the role of organized criminal networks in child abuse and exploitation. Chapter III discusses efforts at combating the problem of ICT-facilitated child abuse and exploitation. It briefly explores national, regional and international efforts in preventing and suppressing the main forms of ICT-facilitated child abuse and exploitation. Chapter III also provides an overview of different practices and policies used to combat ICT-facilitated child sexual abuse and exploitation and identifies opportunities to enhance the fight against these crimes.

[26] UNODC, 2013. Pp. 17-18.
[27] UNODC, 2013. Pp. 18-19.

I. IDENTIFYING AND DESCRIBING THE PROBLEM

This chapter identifies and defines key terms in analysing the problem of ICT-facilitated child abuse and exploitation and describes the most common types and forms of related behaviour. Due to the relatively recent emergence of many forms of cybercrime and ICT-facilitated child abuse and exploitation, a number of definitions and terms are still evolving. While a few terms key terms, such as "child", have clear international legal reference points, others do not. As a result, not all terminology used in this study is intended to be of a definitional character, legal or otherwise. Rather, the study seeks to provide an effective description of relevant phenomena, practices and acts, which may or may not be currently criminalized in all jurisdictions.

Key terms and concepts

Child and children

Article 1 of the Convention on the Rights of the Child (CRC)[28] defines "child" as any person "below the age of eighteen years unless under the law applicable to the child, majority is attained earlier." Importantly, the CRC leaves open the option for States to adopt lower or higher ages of majority, thus giving States Parties some leeway in defining childhood.

Similarly, article 3 *(d)* of the Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children of the United Nations Convention against Transnational Organized Crime defines children as persons under 18 years of age. Article 2 of International Labour Organization (ILO) Convention No. 182 on the Worst Forms of Child Labour conclusively defines children as anyone under the age of 18 years. The 2009 Report of the Executive Director on Effective crime prevention and criminal justice responses to combat sexual exploitation of children,[29] prepared by UNODC for the eighteenth session of the Commission on Crime Prevention and Criminal Justice (CCPCJ), notes that some Member States generally define "child" for the purposes of national child sexual exploitation legislation as any person less than 18 years of age, while others chose to differentiate between distinct categories of minors, such as infants, juveniles, and adolescents, thereby using different age-thresholds. Variations in the definition of "child" under different legal systems is one factor that can complicate the ability of law enforcement agencies and others to intervene in cases of child abuse and exploitation.[30]

Abuse and exploitation

The World Health Organization (WHO), describes "abuse" of children as either the physical, emotional or sexual mistreatment of a child, or the neglect of a child, in the context of a relationship of responsibility, trust or power, resulting in actual or potential harm to the child's physical and/or emotional health, survival and development[31] "Child sexual abuse" can be described, more specifically, as: "[t]he involvement of a child in sexual activity that he or she does not fully comprehend, is unable to give informed consent to, or for which the child is not developmentally prepared and cannot give consent, or that violates the laws or social taboos of society. Child sexual abuse is evidenced by this activity between a child and an adult or another child who by age or development is in a relationship of responsibility, trust or power, the activity being intended to gratify or satisfy the needs of the other person."[32]

[28] Convention on the Rights of the Child. New York, 20 November 1989. United Nations, *Treaty Series*, vol. 1577. To date, the CRC has 194 States Parties, making it one of the most widely ratified international treaties.

[29] E/CN.15/2009/14 Paragraph 4, available at http://www.unodc.org/unodc/en/commissions/CCPCJ/session/18.html.

[30] See Quayle, E., Lööf, L., Soo K., Ainsaar, M., Glossary. In: Ainsaar, M., Lööf, L., (eds.), Online behaviour related to child sexual abuse. Literature Report,. P. 9. Available at http://www.childcentre.info/robert/public/Online_behaviour_related_to_sexual_abuse.pdf.

[31] WHO, 2014. Child maltreatment, Fact sheet N°150. Available at http://www.who.int/mediacentre/factsheets/fs150/en/.

[32] WHO, 2003. Guidelines for medico-legal care for victims of sexual violence. P. 75. Available at http://whqlibdoc.who.int/publications/2004/924154628X.pdf?ua=1.

In this context, "contact" and "non-contact" sexual abuse are frequently distinguished from one another both in terms of the actual conduct, as well as with regards to its criminalization. This is discussed further in chapter III: Combating the problem. Contact sexual abuse is used to refer to in-person sexual contact of a harmful nature. Non-contact sexual abuse denotes the producing, possessing or distributing of sexual abuse material, making harassing or sexually suggestive comments to children, advertising sexual services of children on the Internet, and actively employing or viewing children in live online sex shows.[33]

With respect to "exploitation", the United Nations High Commissioner for Refugees (UNHCR) has described the word "exploiting" to mean "using for one's own profit or for selfish purposes".[34] More specifically, UNHCR describes the "exploitation of a child as the use of the child in work or other activities for the benefit of others and to the detriment of the child's physical or mental health, development, and education".[35] Exploitation thus includes, but is not limited to, child labour and child prostitution. Article 3 *(a)* of the Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children of the United Nations Convention against Transnational Organized Crime (UNTOC) does not define exploitation but includes illustrative forms of exploitation in the definition of trafficking in persons. These include, at a minimum, the exploitation of the prostitution of others or other forms of sexual exploitation, forced labour or services, slavery or practices similar to slavery, servitude or the removal of organs.

Both child sexual abuse and exploitation involve an offender taking advantage of a child's lack of power and status, and can refer to acts that are very similar or offences that overlap. An offender might, for example, sexually abuse a child and then further exploit that child by selling a recording of the abuse. Acknowledging this, the United Nations Children's Fund (UNICEF) has declared that "[s]exual abuse becomes sexual exploitation when a second party benefits—through making a profit or through a quid pro quo—through sexual activity involving a child. This may include prostitution and child pornography."[36] Under this approach, the term "abuse" focuses more on the treatment of the child or victim, while "exploitation" refers more to the benefit of the offender.

Another fundamental distinction can be drawn between commercial and non-commercial child abuse and exploitation. The Stockholm Declaration and Agenda for Action, adopted at the First World Congress against Commercial Sexual Exploitation of Children in 1996, condemns the commercial sexual exploitation of children as "a form of coercion and violence against children [that] amounts to forced labour and a contemporary form of slavery". ILO defines commercial child sexual exploitation as "the exploitation by an adult with respect to a child or an adolescent—female or male—under 18 years old; accompanied by a payment in money or in kind to the child or adolescent (male or female) or to one or more third parties".[37] Hence, commercial sexual exploitation denotes child exploitation that is committed for monetary or other economic profit, while non-commercial exploitation pertains to exploitative acts committed for personal gratification rather than for financial or economic gain.

Though a seemingly clear distinction, the line between these two forms of abuse and exploitation can become blurred where the quest of a perpetrator for personal gratification coincides with obtaining an economic benefit through the abuse. For example, perpetrators may share child sexual abuse material with online community members for personal gratification. As some communities require commercial distribution of abuse material in order to gain entry or to access additional material, however, consumers of child sexual abuse material, could engage in both commercial and non-commercial exploitation through the same act. Similarly, a trafficker might sexually abuse a child that he or she later forces to engage in commercial sexual exploitation.

---

[33] Quayle, E, et al.. *In*: Ainsaar, M., Lööf, L. (eds.). Pp. 10-11. Available at http://www.childcentre.info/robert/public/Online_behaviour_related_to_sexual_abuse.pdf; See also Subgroup Against the Sexual Exploitation of Children, the NGO Group for the Convention of the Right of the Child. 2005. *Semantics or Substance? Towards a Shared Understanding of terminology relating to the sexual abuse and exploitation of children*. P. 41.

[34] UNHCR, 2001. *Action for the Rights of Children. Critical Issues*: *Abuse and Exploitation*.

[35] *Ibid*.

[36] See Subgroup Against the Sexual Exploitation of Children, 2005. P. 16

[37] ILO, *Commercial sexual exploitation of children and adolescents. The ILO's response*. Available at: http://www.ilo.org/ipec/areas/CS-EC/lang--en/index.htm.

Main forms of ICT-facilitated child abuse and exploitation

Not all forms of ICT-facilitated child abuse and exploitation are necessarily new or fundamentally different from existing forms of child abuse and exploitation. In a number of instances, however, ICTs not only facilitate the commission of an abusive and/or exploitative act but also give rise to new types of child sexual abuse and exploitation. Although a consistent typology is still lacking, the main forms of ICT-facilitated child abuse and exploitation can be identified by a survey of practice.[38] For instance, the results of a 2003 survey report carried out by ECPAT International in Thailand found that

> "[c]hildren can be abused through the Internet in two main ways. Firstly, they can be exposed to illegal or other harmful materials which they are ill-prepared to deal with e.g. child pornography, hard-core adult pornography, [...] bomb-making or financial scams. Secondly, children can come into direct contact with, and possibly fall prey to, sexual exploiters. Very often those who publish harmful or illegal material, such as child pornography, and those seeking to make contact with children through the Internet for illegal or improper ends, are one and the same. [39]

Similarly, a 2006 study based on research findings and police practices in the United States, the United Kingdom, Canada, Australia, New Zealand, the Netherlands and Scandinavia conducted by the United States Department of Justice, found that in addition to assisting in the proliferation of child sexual abuse material, the Internet facilitates child sexual abuse by allowing networking among child abuse perpetrators. It can be used to seek out and groom victims, for cyberstalking, as well as to promote child sex tourism and trafficking in children.[40]

The European Union offers three categories to explain forms of behaviour related to ICT-facilitated child abuse and exploitation.[41] The first category is described as online harm from content, which conceives of the child as a passive recipient of pornographic or harmful sexual content. A second category refers to harm from contact, where the child is targeted as a participant by an adult or another child in activities such as sexual abuse that is recorded and then distributed; this category also includes online grooming for sexual abuse or cyberbullying. The third category refers to harm from conduct, where the child actively initiates risky online behaviour including the production of self-generated content, bullying others or physically meeting online "friends".

Overall, while generic categories can be identified, it is clear that there is fluidity between types of offending behaviours, with some actions capable of falling in more than one category. A number of attempts, including that of the EU Safer Internet Project ROBERT,[42] reproduced in figure II below, have been made to classify the main forms of Internet-facilitated child sexual abuse, and their relation to each other from a typological perspective.

[38] UNODC, 2013. Chapter Four (Criminalization).

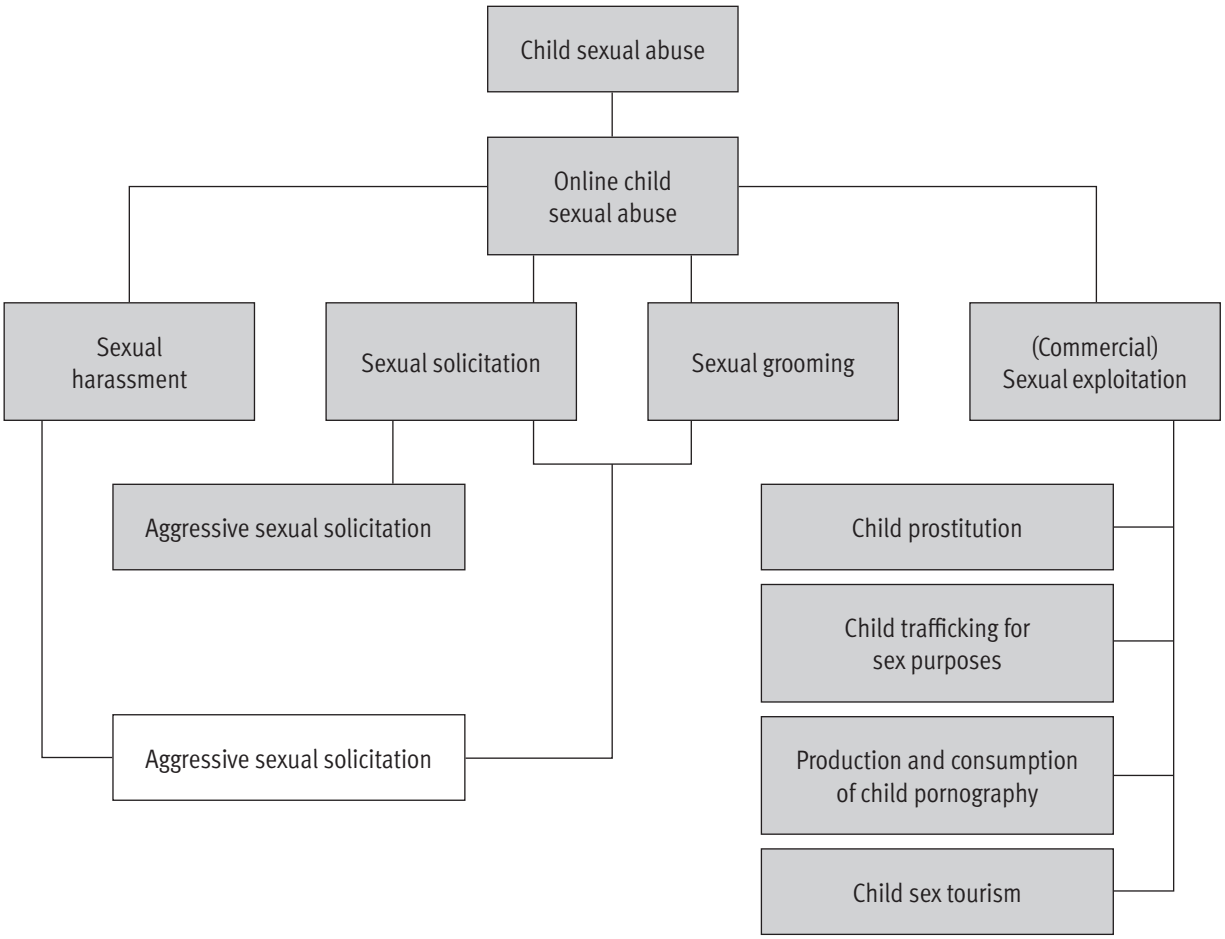
[39] Michelet, I., 2003. P. 2.

[40] U.S. Department of Justice, Community Oriented Policing Services, 2006. *Child Pornography on the Internet*. P. 21.

[41] Livingstone S., Haddon, L., 2009. *EU Kids Online final Report*. P.10: also cited in UNICEF, 2011.

[42] Quayle, E., et al. In: Ainsaar, M., Lööf, L. (eds). P. 16.

Figure II. Forms of Internet-facilitated child sexual abuse



Source: EU Safer Internet Project.

Taking such work into account, and drawing from available research and data, including the Cybercrime Study, the present study considers the main forms of ICT-facilitated child abuse and exploitation under the following broad headings: child sexual abuse material (child pornography); commercial sexual exploitation of children; cyberenticement, solicitation and grooming; cyberbullying, cyberharassment and cyberstalking; and exposure to harmful content.

Child sexual abuse material (child pornography)

Before elaborating on the different forms of child sexual abuse material, it is important to first describe the term itself.

Article 2 *(c)*, Optional Protocol to the CRC on the sale of children, child prostitution, and child pornography describes child pornography as "any representation, by whatever means, of a child engaged in real or simulated explicit sexual activities or representation of the sexual parts of a child, the dominant characteristics of which is depiction for a sexual purpose." Article 34 of the CRC itself requires States Parties to take all appropriate national, bilateral and multilateral measures to prevent the "exploitative use of children in pornographic performances and materials."[43] Article 9 (2) of the Council of Europe Convention on Cybercrime defines "child pornography" as including "pornographic material that visually depicts: *a)* a minor engaged in sexually explicit conduct; *b)* a person appearing to be a minor engaged in sexually explicit conduct; *c)* realistic images representing a minor engaged in sexually explicit content". Non-governmental organizations

[43] Subgroup Against the Sexual Exploitation of Children, 2005. P. 26.

have also proposed definitions, such as the "visual depiction of a child engaged in explicit sexual conduct, real or simulated, or the lewd exhibition of the genitals intended for the sexual gratification of the user, and involves production, distribution and/or use of such material."[44]

While the term "child pornography" is still widely used, "child sexual abuse material" has been increasingly used to describe sexually explicit representations of children, as the term is believed to more accurately reflect the grave nature of the content and to challenge any notion that such acts might be carried out pursuant to the consent of the child.[45] The COSPOL Internet Related Child Abusive Material Project (CIRCAMP), for example, advocates the notion that "[a] sexual image of a child is 'abuse' or 'exploitation' and should never be described as 'pornography'. Pornography is a term used for adults engaging in consensual sexual acts distributed legally to the general public for their sexual pleasure. Child abuse images are not. They involve children who cannot and would not consent and who are victims of a crime."[46] Indeed, from a law enforcement perspective, child sexual abuse material is documented evidence of the crime of sexual abuse or rape in progress.[47]

Child sexual abuse material comes in many forms, including photographs, negatives, slides, magazines, books, drawings, movies, videotapes and computer disks or files.[48] In essence, however, child sexual abuse material consists of a recording, usually in still or video, which depicts a child engaged in sexually explicit activity.[49] While the term "child pornography" is the one most commonly used in legal definitions and in international policy documents, this study preferentially uses the term "child sexual abuse material" for the reasons set out above.

Commercial sexual exploitation of children

Advances in technology have become instrumental in the commercial sexual exploitation of children, including trafficking in children for the purposes of sexual exploitation, and the abuse and exploitation of children in the travel and tourism industries.

International law defines trafficking in persons as "the recruitment, transportation, transfer, harbouring or receipt of persons, by means of the threat or use of force or other forms of coercion, of abduction, of fraud, of deception, of the abuse of power or of a position of vulnerability or of the giving or receiving of payments or benefits to achieve the consent of a person having control over another person, for the purpose of exploitation."[50] In this context, it is important to note that the recruitment, transportation, transfer, harbouring or receipt of a child for the purpose of exploitation shall be considered trafficking in persons, even if it does not involve any means of threat or use of force or other forms of coercion, abduction, fraud, deception or the abuse of power or of a position of vulnerability or the giving or receiving or payments or benefits.[51]

Article 2 *(b)* the Optional Protocol to the CRC on the sale of children, child prostitution and child pornography defines the prostitution of children as the use of children in sexual activities for remuneration or any other form of consideration. This definition provides detail for the purposes of article 34 of the CRC, which obliges States Parties to take measures to prevent the exploitative use of children in prostitution or other unlawful sexual practices. By its nature, prostitution of children involves someone other than the child benefiting from a commercial transaction in which the child is made available for sexual purposes.[52] The terms, "child prostitution" and "the prostitution of children," are often used interchangeably with "the commercial sexual exploitation of children". Technically, however, sexual exploitation encompasses a broader array of commercial offences in addition to the prostitution of children and may include child marriage, domestic labour and the trafficking of children for sexual purposes.[53]

[44] *Ibid*. P. 33.

[45] Quayle, E., et al. In: Ainsaar, M., Lööf, L. (eds.). P. 12.

[46] COSPOL Internet Related Child Sexual Abuse Material Project www.circamp.eu/index.php?option=com_content&view=article&id=10:child-pornography-versus-child-sexual-abuse-material

[47] *Ibid*.

[48] http://www.ecpat.org.nz/Resources/FAQ.aspx#_Anchor11.

[49] See www.inhope.org/gns/Internet-concerns/overview-of-the-problem/child-pornography.aspx.

[50] United Nations, *Treaty Series*, vol. 2237.

[51] Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, supplementing the United Nations Convention against Transnational Organized Crime. Article 3 *(c)*.

[52] Subgroup Against the Sexual Exploitation of Children, 2005. P. 13.

[53] Quayle, E., et al. In: Ainsaar, M., Lööf, L. (eds.).

Another major form of commercial sexual exploitation of children is abuse and exploitation in the travel and tourism industries. This is also commonly referred to as "child sex tourism" and may be described as:

> "…the commercial sexual exploitation of children by men or women who travel from one place to another, usually from a richer country to one that is less developed, and there engage in sexual acts with children, defined as anyone under the age of 18. Child sex tourism takes various forms, but generally it is about adult men who, in the course of travelling away from home, pay in cash or kind for sex with children."[54]

Child sex tourists may be either "preferential" abusers, who deliberately seek out children for sex, or "situational" abusers, who take advantage of an opportunity or a feeling of anonymity afforded by travelling.[55] A more detailed description of offender profiles is contained in chapter III (Combating the problem).

Cyberenticement, solicitation and online grooming

The terms "cyberenticement", "solicitation" and "online grooming" are commonly used collectively or interchangeably to describe communications made by adults through the use of ICTs for the purpose of sexually abusing or exploiting minors. In the United States, for example, many states have adopted legislation related to cyberenticement that seeks to criminalize attempts at knowingly soliciting a minor to engage in sexual activity by communicating through the Internet. Such statutes "come in a variety of forms but generally punish any person who (1) uses a computer or similar device (2) to contact a person whom he knows or believes to be a minor (3) to solicit, encourage, entice, or lure him or her (4) for the purposes of engaging in sexual activity in violation of state laws."[56]

Within the European Union, "solicitation of children for sexual purposes" refers to the intentional proposal, through information and communication technologies, by an adult, to meet a child who has not reached the age of majority under domestic law, for the purpose of committing sexual abuse or producing child pornography where this proposal has been followed by material acts leading to such a meeting.[57] Sexual solicitation may also refer to "requests [to a child] to engage in sexual activities or sexual talk or give personal sexual information that are unwanted or, whether wanted or not, made by an adult."[58]

"Grooming" can be considered as conduct that takes place as part of cyberenticement or prior to solicitation. It refers to a series of actions that facilitate cyberenticement or solicitation deliberately undertaken with the aim of befriending and establishing an emotional connection with and gaining the trust of a child, in order to lower the child's inhibitions in preparation for sexual activity with the child.[59] The preparation element of the conduct can be described as "a process by which a person prepares a child, significant adults and the environment for the abuse of this child. Specific goals include gaining access to the child, gaining the child's compliance and maintaining the child's secrecy to avoid disclosure."[60] Grooming "may take minutes, hours, days or months, depending on the goals and needs of the abuser and reactions of the young person."[61]

---

[54] Subgroup Against the Sexual Exploitaiton of Children, NGO Group for the Convention of the Right of the Child, 2005. Pp. 18-19.

[55] ECPAT. End Child Prostitution, Child Pornography and Trafficking of Children for Sexual Purposes. Available at: http://www.ecpat.net/faqs#child-sex-tourism; see also Kinnear, K. L., 2007. *Childhood Sexual Abuse* (2nd ed.). P.7.

[56] Sorenson Stanger, J., 2005. "Salvaging States' Rights To Protect Children from Internet Predation: State Power To Regulate Internet Activity Under the Dormant Commerce Clause", *Birmingham Young University Law Review*, 2005:191. Available at: http://digitalcommons.law.byu.edu/lawreview/vol2005/iss1/4

[57] Art. 6, Directive 2011/92/EU of the European Parliament and the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA [L 335/1 2011]. See also article 23 Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse.

[58] Quayle, E., et al. In: Ainsaar, M., Lööf, L. (eds.). P. 12.

[59] Gillespie, A., 2002. "Child protection on the Internet challenges for criminal law", *Child and Family Law Quarterly*, 14:411.

[60] Quayle, E., et al. In: Ainsaar, M., Lööf, L. (eds.). P. 15.

[61] UNICEF, 2011. P.2.

Cyberbullying, cyberharassment and cyberstalking

ICTs can also facilitate an array of other problematic conduct within which the lines between various forms of potentially abusive or abuse-related conduct can be difficult to discern, and which may or may not amount to a criminal offence. Conduct such as cyberharassment, for example, refers to the intimidation, repeated or otherwise, of one individual by another or by a group, perpetrated through or utilizing electronic means.[62] Some approaches emphasize the threatening aspects of the conduct, defining the term as online conduct that "involves threats or other offensive behaviour, sent online to the youth or posted online about the youth for others to see."[63] Other approaches emphasize the elements of aggression and the potential for harm: "online harassment occurs when someone uses the Internet to express aggression towards another person. This can take the form of inflammatory e-mails or instant messages, or damaging pictures or text posted on a profile".[64]

Cyberharassment may escalate to extortion or even kidnapping. Sex-related extortion on the Internet, sometimes known as "sextortion", is becoming increasingly common. In such cases, offenders use information and photos, including collected through online contact with the victim, to blackmail minors into producing sexually explicit content or meeting them for sexual purposes, sometimes even threatening victims and their families. Offenders may send harassing messages or even threats via e-mail, instant message, social media profiles or other simple forms of electronic communication. Offenders may also post images of the victim juxtaposed on pornographic images from other sources or develop a whole website or social media page focused on their victims. Other tactics consist of provoking attacks on victims by a third-party or contacting the victims' friends, family, teachers or employers.

Similarly to cyberharassment, cyberbullying encompasses the use of ICTs to harm a victim or victims in deliberate, repeated, and hostile ways. This can include but is not limited to the use of the Internet, cell phones or other devices to send or post text or images intended to hurt or embarrass another person.[65] As noted in a 2011 UNICEF study conducted in South Africa on the use of social networks, "[even] though bullying is a phenomenon that existed well before the creation of the World Wide Web, the Internet, in addition to mobile phones, has magnified the problem by creating a new venue through which bullying can be executed. When perpetrated online, cyberbullying is eased by the apparent anonymity and distance from the victim."[66] Some approaches to characterizing the phenomenon are centered around the age of the victim and perpetrator, such as when a child, pre-teen or teen is tormented, threatened, harassed, humiliated, embarrassed or otherwise targeted by another child, pre-teen or teen using the Internet, interactive and digital technologies or mobile phones.[67] In cyberbullying, "the identity of the bully may or may not be known. Cyberbullying can occur through electronically-mediated communication at school; however, cyberbullying behaviours commonly occur outside the school as well."[68]

"Cyberstalking" is commonly understood as a course of action that involves more than one incident perpetrated through or utilizing electronic means that causes distress, fear or alarm. It is primarily characterized by the repetitive aspect of the conduct at hand.[69] Just like its offline counterpart, cyberstalking includes activities related to locating, surveying, and harassing or manipulating victims. Compared to spatial or offline stalkers, however, cyberstalkers are characterized by use of online sources of information and means of contacting victims.[70] The nature of online communication and the vast amount of information that stalkers can access online may result in a false sense of intimacy for the

[62] Maple, C., Short, E., Brown, A., 2011. *Cyberstalking in the United Kingdom. An Analysis of the ECHO Pilot Survey*. University of Bedfordshire – National Centre for Cyberstalking Research. P. 4. Available at: http://www.beds.ac.uk/__data/assets/pdf_file/0003/83109/ECHO_Pilot_Final.pdf.

[63] Mitchell, K., Finkelhor, D., Wolak J., 2000. *Online victimization: A report on the nation's youth*. Alexandria, VA: National Center for Missing and Exploited Children. Available at: http://www.unh.edu/ccrc/pdf/Victimization_Online_ Survey.pdf

[64] Ybarra, M., Espelage, D., Mitchell, K., 2007. "The Co-occurrence of Internet Harassment and Unwanted Sexual Solicitation Victimization and Perpetration: Associations with Psychosocial Indicators", *Journal of Adolescent Health*, 41:32; see also Quayle, et al. In: Ainsaar, M., Lööf, L. (eds.). P. 15.

[65] http://stopcyberbullying.org/what_is_cyberbullying_exactly.html.

[66] UNICEF, 2011. *From 'What's your ASLR' to 'Do You Wanna Go Private?'*. P. 12. Available at: http://www.unicef.org/southafrica/SAF_resources_mxitstudy.pdf.

[67] http://stopcyberbullying.org/what_is_cyberbullying_exactly.html

[68] Quayle, E., et al. In: Ainsaar, M., Lööf, L. (eds.). P. 13.

[69] See e.g. U.S. Department of Health & Human Services, 2011. What is Cyberbullying. Available at: http://www.stopbullying.gov/cyberbullying/what-is-it/. See also Maple, C., Short, E., Brown, A., 2011. P. 4.

[70] Maple, C., Short, E., Brown, A., 2011. P. 13.

offender and the relative anonymity afforded by the virtual context can have a disinhibiting effect.[71]

Exposure to harmful content

"Exposure to harmful online content" pertains to situations where a child accidentally or intentionally views pornographic or other content that is judged to be harmful to their development, sexual or otherwise. Harmful content can cover a broad range of audio, visual or written content and other material that has the ability to negatively influence children, although not necessarily illegal in itself. Examples include online pornography; violent video games; websites that espouse racial or ethnic hatred; commercial sites that seek to swindle youth or steal their identities; and, especially, sexual material.[72] Children may be exposed to harmful content as the result of deliberate searches or of inadvertent contact resulting from search queries, pop-up advertisements or emails received from spam operators.

Children who accidentally come across harmful content can be affected before they determine whether the content is appropriate or take action to remove themselves from the situation. Some children can experience signs of stress from the exposure, while others may not externally appear to be affected. Some children's exposure may spark curiosity to seek more information or materials. Other children are naturally curious and may intentionally seek out information on the Internet in the first place. In either case, exposure to explicit or harmful content has the potential to influence the child's development of values and perceptions. While some websites and games use age restrictions and checks to ensure that children are not exposed to harmful content, often there are few real barriers to prevent children from accessing such content at a younger age.[73]

Exposure to online pornography is particularly prevalent among male adolescents. As noted in a UNICEF study on child safety online, ICTs have created an environment in which pornography has become easily accessible, with many available sites displaying extreme forms of pornography that can be accessed by young people, including through unsolicited exposure.[74] A 2006 telephone survey in the United States among a sample of 1,500 youth Internet users aged 10 to 17 years found that, out of 42 per cent of children between the ages of 10 and 17 years who reported previous exposure to pornographic content, 66 per cent indicated that the exposure had been unwanted. The survey also revealed that children who have been harassed, bullied or propositioned for sexual encounters are more likely to experience unwanted exposure to harmful content, suggesting a link between various forms of harmful conduct and indicating that some children are repeatedly victimized.[75]

---

[71] University of Houston, Stalking and Cyberstalking. Available at http://www.uh.edu/wrc/safety-and-violence-prevention/stalking%20/index.php.

[72] U.S. Children's Internet Protection Act Secs. 1703*(b)*(2), 20 U.S.C. sec 3601*(a)*(5)(F) as added by CIPA sec 1711, 20 U.S.C. sec 9134*(b)(f)*(7)(B) as added by CIPA sec 1712*(a)*, and 147 U.S.C. sec. 254*(h)(c)*(G) as added by CIPA sec. 1721*(a)*; See also http://www.vodafone.com/content/parents/get-involved/inappropriate_harmful_ content.html.

[73] Mitchell, K., Finkelhor, D., Wolak, J., 2003. "The Exposure of Youth to Harmful Content on the Internet. A National Survey of Risk, Impact and Prevention", *Youth and Society* 34:332 s. Available at: http://www.unh.edu/ccrc/pdf/Exposure_risk.pdf

[74] UNICEF, 2011. P.2.

[75] Mitchell, K., Finkelhor, D., Wolak, J.,2007. "Unwanted and Wanted Exposure to Online Pornography in a National Sample of Youth Internet Users". *Pediatrics* 119:247.

II. EVALUATING THE PROBLEM

The advent of ICTs has led to a continuum of effects on the abuse and exploitation of children. Some conduct facilitated by ICT, particularly crimes involving contact sexual abuse, shares many features and similarities with forms of non-technology facilitated abuse and exploitation, and can be countered with similar methods. In some instances, the effect of technology on an existing form of abuse and exploitation is so transformational, however, that it must be prevented and countered in new ways. In a few cases, the use of new information and communication technologies has given rise to completely new forms of child abuse and exploitation.

The use of ICTs in the commission of offences can increase levels of harm to victims, in particular by facilitating the layering and intertwining of offences such that multiple forms of abuse and exploitation facilitated by technology can take place simultaneously or be committed against the same victim over time. The Council of Europe notes, for example, that: "[n]one of these new technologies are in and of themselves harmful" but they—inadvertently—provide criminals with "new, efficient, and often anonymous" ways and means of exploiting children.[76]

This chapter evaluates the effects of ICTs on common forms of child abuse and exploitation. These include increased access to victims and to child sexual abuse material; increased profits obtained by criminal enterprises; reduced risk of identification and prosecution of perpetrators; increased potential levels of harm for victims; and provision of social affirmation for offenders. New forms of child abuse and exploitation enabled by ICTs are also discussed, including made-to-order child sexual abuse material; user-generated and self-generated content including sexting; and the broadcasting of live sex abuse.

In addition, this chapter provides a brief overview of the main risk factors for victims as well as possible offender profiles. With regard to the identification of potential victims, the relevant factors discussed include gender and sexual orientation; prior abuse and family dysfunction; poverty and migration; age; online behaviour; and social isolation. With regard to offender profiling, general profiles and motivations of offenders, as well as common offender characteristics, are discussed, including gender; age; other demographic characteristics; and technological sophistication.

Finally, this chapter briefly describes organized groups of offenders and the role of organized criminal networks in child abuse and exploitation.

Effects of ICT on common existing forms of child abuse and exploitation

Enhanced access to victims and to child sexual abuse material

Offenders are able to gain easier access to larger and new populations of children through the use of online forums, e-mail, social networks and other Internet-based communication tools. Offenders may, for example, simultaneously have up to 200 "friends" or more with whom they are at different stages of grooming.[77] With such a large pool of potential victims, offenders can take calculated risks by initiating sexual conversations with children and gauging their reaction.[78] Offenders may then focus on those children that respond favourably, or at least remain engaged, thus enabling them to allocate their time to higher probability targets. Analysis from Statistics Canada suggests that following the addition of new child luring through the Internet offences in the Canadian Criminal Code in 2002, the number of incidents reported to the police increased. The number of police-reported child luring incidents in 2006 was 1.5 times greater than in 2005, and rose

[76] Council of Europe, 2003. Group of Specialists on the Impact of the Use of New Information Technologies on Trafficking in Human Beings for the Purpose of Sexual Exploitation [EG-S-NT (2002) 9 rev.]. Available at http://www.coe.int/t/dghl/monitoring/trafficking/docs/activities/EGSNT2002-9rev_en.asp.

[77] Webster, S. et al, 2010. *Scoping Report: European Online Grooming Project*. Pp. 13-14.

[78] Choo, K. R., 2009, *Online Child Grooming: A Literature Review on the Misuse of Social Networking Sites for Grooming Children for Sexual Offences*. Australian Institute of Criminology. Pp. 11-16.

another 31 per cent in 2007.[79] While this may be indicative of a genuine underlying increase in such acts, police-recorded crime statistics are a function of both the number of actual acts, as well as awareness of the criminal nature of the act, and willingness to report. While Statistics Canada notes that "[it] is difficult to know to what extent the growth in child luring offences reported to police may be related to increased efforts to raise public awareness or to other factors, such as advances in police efforts to capture online predators, or to an increase in the number of luring incidents", it nonetheless concludes that "growing access to technology may increase the risk of online sexual exploitation of children and youth."[80]

ICTs also enable perpetrators to have increased access to information about victims. Social networking sites can host enormous quantities of freely shared personal and biographical information. An inherent risk of such information sharing is the fact that children often lack discretion and rely on a false sense of privacy and safety. Even children who do attempt to protect their privacy and security regularly struggle to keep abreast the frequently changing privacy rules of social network sites. New features in social networking-sites such as geotagging of images and "checking-in" to places via mobile devices can further enhance offenders' knowledge of a child's location.[81]

Services and applications are available which make it easier for offenders to gather personal information about their prospective victims. For example, the "cree.py tool" extracts information associated with a single e-mail address from diverse social networking sites, providing the user with a dossier of information on potential victims, including geolocation data when available. In addition to publicly available information, and while most sites and applications increasingly employ extensive cybersecurity, personal information always risks compromise through hacking and other forms of illegal access.[82]

ICT may further facilitate access to child victims for the purposes of human trafficking. Perpetrators may recruit new victims, including children, through websites, as well as by using social media technology to advertise their services to a broad public. The 2013 United States Global Report on Trafficking in Persons, for example, made special note of the impact of technology on recruitment of trafficking victims:

> "In the fight against modern slavery, technology can be a double-edged sword. Traffickers use technology to advertise their services widely and develop new methods to recruit, manipulate, and lure potential victims. Meanwhile, governments, anti-trafficking advocates, and technology companies are collaborating to leverage technological tools to turn the tables on the traffickers."[83]

Similarly, child sex tourists may use chat rooms, message boards, peer-to-peer file-sharing servers, news groups, and specialized websites to obtain information on potential victims and destinations, share stories, trade child sexual abuse material, and plan travels.[84] Some reports suggest that technology is the engine behind a growth in the sex trade, and that extensive use of the Internet for marketing sex tours is consonant with overall Internet usage in a country.[85]

In the process of accessing child victims through online contact, offenders may use ICTs to break down both physical and psychological barriers to abusing or exploiting children. For example, many social networking sites effectively enable users to cover or hide their true identities, allowing perpetrators to easily adopt false identities in order to lure children into an online relationship. Once children feel emotionally attached and begin to trust offenders, perpetrators may more easily reveal their true identities, while still maintaining the loyalty of their victims.[86]

Offenders may also make use of pornography or child sexual abuse material to remove psychological barriers by convincing their targets that child abuse is "normal." Offenders

---

[79] Statistics Canada, 2009. *Child Luring Through the Internet*.

[80] *Ibid*. P.6 and P.9.

[81] See Livingstone, S., Olafsson, K., Staksrud, E., 2011. Social networking, age and privacy. EU Kids Online. Available at http://eprints.lse.ac.uk/35849/1/Social%20networking%2C%20age%20and%20privacy%20%28LSERO.pdf; see also Choo, K. R., 2009. Pp. 16-18.

[82] Ibid.

[83] U.S. Department of State, 2013. Trafficking in Persons Report. P. 14. Available at http://www.state.gov/documents/organization/210737.pdf.

[84] U.S. Department of State, 2007.Trafficking in Persons Report. P. 23. Available at http://www.state.gov/documents/organization/82902.pdf#page=25&zoom=auto,0,477.

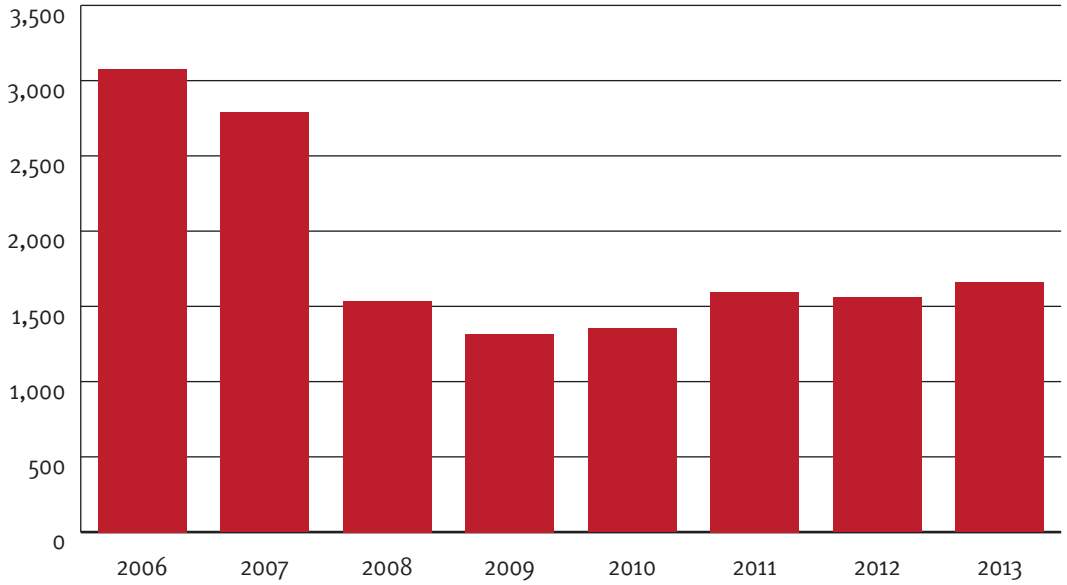
[85] Shared Hope International, 2007. Demand: A Comparative Examination of Sex Tourism and Trafficking in Jamaica, Japan, the Netherlands, and the United States. Available at http://sharedhope.org/wp-content/uploads/2012/09/DEMAND.pdf; Jamaican sex markets lag behind those in the other countries in the use of the Internet to advertise and promote its thriving local commercial sex markets, most likely because of the limited use of the Internet within the country.

[86] See *ibid*. P. 12; see also UNICEF, 2011. P. 5.

may try, for example, to use sexual abuse materials to validate and vindicate acts such as rape, battery, sexual harassment, prostitution or child sexual abuse.[87] By providing channels for fast, free and difficult-to-trace content, ICTs have provided offenders with increased opportunities to expose children to such harmful content. A particular source of unwanted harmful content involves the transfer of peer-to-peer files. Offenders may mislabel such files containing, for instance, violent child sexual abuse material, in order to trick children into opening, downloading and viewing them.

In addition, file transfer services through e-mail, instant messaging, social networking sites, file transfer protocols, cloud computing and do-it-yourself websites have dramatically increased the accessibility of child sexual abuse material. It is estimated that from 1997-2006, the number of child pornography images on the Internet increased by 1,500 per cent. In 2001, the CyberTipline mandated by the United States Congress received 21,603 reports of child pornography. In 2004, the number increased by 491 per cent to 106,176 reports of child pornography on the Internet.[88] As illustrated in figure III, data from the Internet Watch Foundation (IWF) identified 13,182 webpages containing child sexual images, hosted on 1,660 domains worldwide in 2013.[89]

Figure III. The number of domains hosting child sexual abuse content, by year



Source: Internet Watch Foundation.

[87] Choo, K. R., 2009. Pp. 13 -14.

[88] Mattar, M. Y., 2006. *Protecting Children: The Battle against Child Pornography and Other Forms of Sexual Exploitation*. Statement at U.S. Congressional Hearing before the Commission on Security and Cooperation in Europe (Washington, DC, September 27, 2006). Available at http://www.csce.gov/index.cfm?FuseAction=ContentRecords.ViewWitness&ContentRecord_id=774&ContentType=D&ContentRecordType=D&ParentType=H&CFID=15055102&CFTOKEN=d2f0d82887026b5b-5B6D99F3-9100-FBB0-C72DC9EBC4DA7CFE.

[89] IWF, 2014. Annual & Charity Report 2013. P. 11. Available at https://www.iwf.org.uk/accountability/annual-reports/2013-annual-report.

Recent estimates have indicated that the majority of child sexual abuse material is now exchanged via non-commercial channels, specifically public peer-to-peer platforms, such as Gnutella, eDonkey and eMule. Private peer-to-peer networks are often used by mid-level offenders who establish closed groups to exchange encrypted files. Anywhere from 7.5 to 24 per cent of child sexual abuse material is currently exchanged via commercial channels. As credit card payments are known by most offenders to risk identification, new and therefore more valuable, abuse material has become a sort of currency in itself, being often used as "payment" for access to other material. While commercial distribution has not been completely eradicated, a trend in decreasing identification of available commercial sexual abuse material may also be due to commercial distributors moving to new platforms or "dark web" environments such as Tor.[90]

Increased profits for criminal enterprises

Advances in ICTs have enabled criminal enterprises that sexually abuse and exploit children to lower operating costs and increase profits. Prior to the widespread availability and use of ICTs, producers of child sexual abuse material had to employ expensive filming and copying equipment, and ship videotapes or CD-ROM copies for distribution and to produce advertising material accordingly. Due to the public nature of such advertisements, offenders used cryptic language and terms so as not to alert law enforcement authorities, which often served to restrict the distribution and profit of such material.

In the current technological context, ICTs markedly reduce the costs and efforts at all stages of the production and distribution of child sexual abuse material. While digital equipment creates a comparatively cheap and easily accessible means of producing and widely distributing child sexual abuse material through the Internet, commercial spam campaigns reduce the challenges and costs related to advertising, enabling child abuse and exploitation networks to quickly expand the scope and scale of their activities. Once directly connected to customers and consumers, providers can continuously advertise additional illicit materials in open and explicit language and keep in touch freely, thus enabling them to generate greater revenue from their activities.

The creation of websites has also become significantly easier in recent years, such that providers of child sexual abuse material no longer have to rely on and hire HTML-programmers and can instead establish a site themselves, either on the public web or, more commonly, on Tor or dark web. With even less effort and expense, and some basic precautions, child sexual abuse material providers can employ photo-sharing, banner advertising and social networking applications to host graphic child sexual abuse content.

The cost-saving effects of ICTs also facilitate child commercial sex trafficking operations. For instance, traffickers are able to recruit, advertise, organize and communicate primarily, or even exclusively, via mobile phone or devices such as tablets, effectively streamlining their activities and expanding their networks. At the same time, operators of illicit businesses are frequently able to charge travelling offenders more money for the service of facilitating encounters at almost any time, and on short notice—a "service" which is facilitated by ICTs.[91]

Reducing offenders' risk of detection

The use of ICTs in the sexual abuse and exploitation of children has also reduced the risk of detection. The use of mobile phones and devices, e-mail and messaging applications can enable perpetrators to hide their identities and obfuscate their activities. Potential offenders can utilize disposable phones or pre-paid SIM cards that, in some countries, do not require any form of registration, to carry out any form of child abuse and exploitation. E-mail accounts may also be registered using false identities, multiple proxies, and public wireless hotspots, making it extremely challenging to link an account-registration with a particular individual. Additionally, many Internet cafés offer reasonable anonymity, as they do not require identification to log on to computers, do not use monitoring systems of any kind, and are unable to enforce codes of conduct.[92]

ICTs can also expand the territorial range and reach of child sexual abuse material distribution, as such material may

[90] EUROPOL. European Cybercrime Centre (EC3), 2013. *Commercial Sexual Exploitation of Children Online: A Strategic Assessment.* Available at https://www.europol.europa.eu/sites/default/files/publications/efc_strategic_assessment__public_version .pdf.

[91] Hughes, D., 2002. "The Use of New Communications and Information Technologies for Sexual Exploitation of Women and Children", *Hastings Women's Law Journal* 13:129-148; Trinidad, A.C. 2005. *Child Pornography in the Philippines*. UP Center for Integrative and Development Studies/UNICEF Manila. Pp. 31-37.

[92] U.S. Department of Justice, 2010. "The National Strategy for Child Exploitation Prevention and Interdiction. A Report to Congress", Pp. 25-26; see also Armstrong H. L., Forde, P.J., 2003. Internet anonymity practices in computer crime. *Information Management & Computer Security* 11:209-215.

be both recorded and distributed solely using mobile telephones or devices. Similarly, by using ICTs, cyberstalkers, harassers and bullies can abuse their victims with less effort and lower risk of detection.[93] Child sex tourists can make use of cloud computing to store images or videos of their encounters, avoiding the risks associated with physically transporting child sexual abuse material through airports and other checkpoints. Moreover, mobile telephone technology connects organizers, victims and consumers of child sexual exploitation and abuse, thus reducing the need for producers and distributors to be physically present at transactions, which in turn serves to better insulate them from detection.[94]

Whereas encryption measures were previously not widespread among producers, distributors and consumers of child sexual abuse material—due to fears of being inadvertently locked out of their collections—many offenders now use both local and remote storage services that include built-in encryption technology to evade detection and complicate the work of law enforcement agencies.[95] Providers and consumers of child sexual abuse material may also have access to new technologies that reduce permanent digital evidence. Applications such as "SnapChat" and "Wickr", for example, enable users to distribute temporary images that disappear within seconds following receipt.[96]

Increased levels of harm for victims

The use of new ICTs in the abuse and exploitation of children has also served to increase levels of harm suffered by victims. Technologies such as peer-to-peer file sharing have escalated the distribution of child sexual abuse material to such an extent that collections consisting of millions of images are commonplace. Cloud-computing technology similarly enables private access to storage that can host massive collections at a very low cost.[97]

With regard to contact sexual abuse, experts have found that a "layering of harms" can occur when images or video of abuse have been distributed online. The contact sexual abuse constitutes the first layer of harm, and the production of an image or video—which exacerbates the negative effects of the abuse—represents a separate, second layer of harm. Each subsequent viewing or distribution of that material serves to re-victimize and thus further exacerbate the psychological damage to the abused.[98]

Ever-increasing levels of violence and a continuously decreasing age of victims in child sexual abuse material have also been observed. Between 2011 and 2012, it is estimated that there was a 70 per cent increase in child sexual abuse material focused on girls under the age of 10, with abuse material involving toddlers or babies not being uncommon.[99] Moreover, a significant number of online forums and channels openly advertise videos of brutal sexual assault.[100]

The increasingly large amounts of readily available online child sexual abuse material also serve to desensitize viewers, resulting in a demand for ever more extreme material.[101] In comparative research on persons possessing child sexual abuse material in the United States between 2000 and 2005, the 2005 group of child sexual abuse material-users had larger quantities of videos than still images, as well as more materials depicting victims under the age of three. The same research noted that in 2005, more consumers used peer-to-peer file sharing than had done so in 2000. In fact, the use of peer-to-peer in the context of child sexual abuse material has been

[93] U.S. Department of Justice, 2010. Pp. 25-26; see also CEOP, 2009. *Strategic Assessment 2008-2009*. Available at: http://ceop.police.uk/Documents/strategic_overview_2008-09.pdf

[94] Shared Hope International, 2007.

[95] Bose, A., 2013. *Commentary at the Informal Expert Group Meeting on the Effects of Information and Communication Technologies on the Abuse and Exploitation of Children*. Vienna. September 23, 2013 through September 26, 2013.

[96] Henn, S., 2013. *Teens Dig Digital Privacy if SnapChat is any Indication*. Available at http://www.npr.org/blogs/alltechconsidered/2013/12/10/249731334/teens-dig-digital-privacy-if-snapchat-is-any-indication.

[97] Bose, A., 2013.

[98] Hamilton, M. Amicus Brief of the American Professional Society on the Abuse of Children in Support of Respondent Amy Unknown in *Doyle Randall Paroline v. Amy Unknown and United States*, U.S. Supreme Court Case No. 12-8561. Available at http://sol-reform.com/12-8561-bsac-APSAC.pdf; see also Wolak, J., Finkelhor, D., Mitchell, K., 2011. "Child Pornography Possessors: Trends in Offender Case Characteristics", *Sexual Abuse: A Journal of Research and Treatment*. 23:22-42 (Noting the increase in Child Pornography possessors increased collection of materials depicting children under years between 2000 and 2006).

[99] CEOP, 2013; Bose, A., 2013. Commentary at the Informal Expert Group Meeting on the Effects of Information and Communication Technologies on the Abuse and Exploitation of Children. Vienna. September 23, 2013 through September 26, 2013.

[100] See e.g. Timberg, C., 2013., How violent porn site operators disappear behind Internet privacy protections. *The Washington Post*. December 6, 2013. Available at http://www.washingtonpost.com/business/technology/how-violent-porn-sites-manage-to-hide-information-that-should-be-public/2013/12/06/e0861378-3773-11e3-ae46-e4248e75c8ea_story.html.

[101] Beech, A., et al. 2008. "The Internet and Child Sexual Offending: A Criminological Review", *Aggression and Violent Behaviour*, 13:216-228.

identified as one driving factor behind the trend towards collections of larger quantities of material, as well as material depicting younger victims and higher levels of violence.[102] The prevalence of child sexual abuse material may also fuel a vicious cycle. As new material features increasingly violent imagery with ever younger victims, offenders may seek more extreme material to derive the same levels of gratification from child sexual abuse material. Non-contact offenders who view and trade child sexual abuse material may feel spurred on to abuse children and create abuse material themselves, either during the grooming or the immediate abuse (which may or may not have been initiated online).[103] Recent arrest statistics from the United Kingdom, for instance, suggest that some offenders had watched and had in their possession child pornography before assaulting or even consequently murdering their victims.[104]

With regard to the commercial sexual exploitation of children, developments in mobile communications afford abusers more control over their victims' movements. Not only can perpetrators require victims to call them at the beginning and end of each encounter, but they can also track victim movements by means of global positioning system (GPS) enabled devices. Moreover, the ubiquity of camera-equipped mobile phones and devices makes victims more vulnerable to the recording or live streaming of abuse for distribution, commercial or otherwise.[105]

Concerning cyberenticement, the widespread use of ICTs and the immediacy of online interactions can lead perpetrators to engage in ever more direct contact with and targeting of victims, to the point that they may solicit sexual contact after only a few brief interactions, unconcerned about offending or alienating victims, or resorting to threatening them into compliance.[106] For example, perpetrators may convince children to share a compromising image and then threaten to send it to their parents or to upload it to a public website in order to extort more graphic content or in-person meetings.[107]

The magnitude and pervasiveness of bullying have also been exacerbated in the current technological environment. Bullies use websites and social media to broaden their audience and to increase their impact on victims. Use of the Internet and other ICT platforms enables perpetrators to quickly and easily enlist others to join in bullying the victim.[108] The semi-anonymous nature of the Internet may increase the viciousness of perpetrators and thus aggravate the harm inherent in the initial bullying. Children may feel trapped in a vicious cycle of online abuse. Such abuse often has a continuous nature due to the always "open" nature of Internet connections on personal mobile devices that may be kept on the person of the victim at all times. Victims may also hesitate to confide in their parents because they doubt their level of technical sophistication or fear that they will lose access to their personal devices. In addition, caregivers may have less opportunity to observe online abuse and to intervene than otherwise possible in a physical environment.[109]

With regard to exposure to harmful content, according to an anonymous survey published in the Journal of Adolescent Health in 2009, 55.4 per cent of teens reported that they had visited a sexually explicit website.[110]

Provision of social affirmation for offenders

The use of ICTs affords unprecedented access to social affirmation for offenders. Whereas in the pre-digital era perpetrators who openly discussed these matters would likely have become ostracized from mainstream communities, accepting online communities exist for all areas of abuse and exploitation, particularly with respect to child sexual abuse material and cyberenticement.[111] Such social reinforcement of child abuse and exploitation can be particularly strong due to its immediate and interactive nature.[112] Massive quantities of readily available child sexual abuse material online may create the false impression of social acceptability, which in turn

[102] Wolak, J., Finkelhor, D., Mitchell, K., 2011.

[103] Howitt, D. Sheldon, K., 2007. "The Role of Cognitive Distortions in Paedophilic Offending: Internet and Contact Offenders Compared", *Psychology, Crime, & Law* 13:469-486.

[104] Bose, A., 2013.

[105] U.S. Department of Justice, 2010. P. D-20.

[106] See Choo, K. R., 2009. P. 12.

[107] CEOP, 2013.

[108] Shariff, S., 2011. *Child Safety Online. Defining the Lines on Cyberbullying: Navigating a Balance Between Child Protection, Privacy, Autonomy and Informed Policy*. Available at http://www.unicef-irc.org/research-watch/Child-Safety-Online/839/.

[109] ECPAT International, 2005. *Violence Against Children in Cyberspace*. Pp. 60-64. Available at http://www.ecpat.net/sites/default/files/Cyberspace_ENG_0.pdf

[110] Braun-Courville, D. K., Rojas, M. 2009. "Exposure to sexually explicit web sites and adolescent sexual attitudes and behaviors", *Journal of Adolescent Health*. 45:156-162.

[111] Choo, K. R., 2009. P. 11.

[112] Bromberg, H. Identity, Belonging and Consciousness in Virtual Worlds. In R. Shields (ed.), 1996. *Cultures of the Internet: Virtual Spaces, Real Histories, Living Bodies*.

diminishes offenders' or potential offenders' inhibitions.[113] Online communities also regularly provide forums for sharing strategies to gain access to victims and to evade law enforcement.[114]

Information and communication technologies as a tool for detection

While the use of ICT in crimes against children poses many challenges, including in respect of detection and perpetrator identification, ICT use by offenders can also generate a number of investigative and evidential leads for the criminal justice system. The nature of Internet connectivity and electronic devices means that evidence of the actions of individuals—in the form of audio and written messages, electronic connections, photographs and videos—can be transmitted through networks and platforms owned and operated by multiple individuals. This provides a potentially far greater range of investigative starting points than in "offline" cases of abuse that may involve only a single victim and perpetrator, and perhaps take place only in one physical location.

Skilled digital investigators are increasingly able to acquire electronic evidence of abuse facilitated by ICT, even when perpetrators take careful steps to avoid leaving, or to delete, digital traces. In the same way as with computers, mobile device forensics can often be used to retrieve images and messages that have been deleted from a mobile phone or other devices. Depending upon data retention times, Internet Protocol (IP) connection logs can provide a complete trace of all times, sources and destinations of Internet connections.

In addition, abuse committed using ICT may be more likely to come to the attention of the police in the first instance than abuse committed offline. Some offenders prolifically produce and publicly distribute abuse material. Parents and other caregivers might also discover abuse through digital footprints or images. Some victims themselves may even be more willing to come forward when they know that digital evidence will corroborate their claims. Online victim reporting portals that offer a non-threatening way to report abuse can also be important in contributing to victim reporting.

When such material is encountered or reported, investigators can proactively follow leads to discover abuse, identify victims and provide victim support and assistance. Law enforcement agencies may be more willing to pursue cases if clear digital evidence of the crime confirms its severity and increases the likelihood of a successful prosecution. Law enforcement officers are also increasingly successful in using information gleaned from child sexual abuse material and other digital evidence to identify, rescue and protect child victims who may remain at risk of ongoing sexual abuse.

New forms of child abuse and exploitation

Made-to-order child sexual abuse material

ICTs have enabled "made-to-order" content to become a profitable option for offenders. This form of child exploitation is commonly linked to organized criminal groups and represents a significant and emerging threat.[115] Sometimes also referred to as on-demand, pay-per-view or bespoke material, perpetrators take orders for and can produce videos or images that conform to a customers' specificities regarding age, race, sex and appearance of the victim. Customers may also specify customized physical settings, plot elements or sexual acts. Some require that the child pay homage to them, for example, by saying or displaying a certain name during the course of the abuse.

In one recent case example, a perpetrator from an EU Member State contacted providers of child sexual abuse material in an Asian country. Using chat services and a webcam, the perpetrator issued instructions regarding the particular type of abuse he wanted to watch, paying as little as US$ 25-30 for each 30 minute session of abuse. During the investigation of the case, it was discovered that many of the women from the particular village where the abuse took place were involved in the crimes.[116]

[113] See Wyre, R. Pornography and Sexual Violence: Working with Sex Offenders., In Catherine Itzen (ed.), 1992. *Pornography; Women, Violence and Civil Liberties*. Pp.237-247.

[114] Choo, K. R., 2009. P. 11.

[115] See e.g. Kendall, V., Funk, M., 2012. *Child Exploitation and Trafficking*. P. 21; Palmer, T., Stacey, L., 2004, *Just One Click: Sexual Abuse Of Children And Young People Through The Internet And Mobile Phone Technology*; see also CEOP 2009; Maley, P., 2012. Children abused 'to order' on Skype. The Australian, May 17 2012. http://www.theaustralian.com.au/news/nation/children-abused-to-order-on-skype/story-e6frg6nf-1226358212495#

[116] EUROPOL, European Cybercrime Centre (EC3), 2013.

The demand for new material appears to be reflected in the range of prices observed. While individual video clips can cost as little as US$ 10 each, and subscriptions as little as US$ 50 for 3 months, one video file of new material on demand can cost as much as US$ 1,200.[117]

User-generated content and self-generated content, including "sexting"

User-generated content is content that is self-created and self-published online by Internet users. Common forms of user-generated content include blogs, videos, podcasts, comments on articles, forum commentaries, social media postings, and contributions to wiki sites. In the context of child abuse and exploitation, self-generated content—a subset of user-generated content—comprises images and videos that are produced by and feature children, especially teens.[118]

"Sexting" is a form of self-generated sexually explicit content,[119] which is generally defined as the "exchange of sexual messages or images"[120] that involves "the creating, sharing and forwarding of sexually suggestive nude or nearly nude images" through mobile phones and/or the Internet.[121] Such material typically involves minors and can be conceived of as "self-produced child pornography".[122] Quantitative research on sexting has found rates of use as wide as 15 per cent to 40 per cent among young people.[123] Motivations for sexting cover a broad spectrum ranging from naive expressions of newfound sexuality to coercion.[124] According to one study, sexting-messages may have an especially coercive impact resembling harassment and bullying or resulting in physical violence.[125]

Mass availability of ICTs has increased the production of and loss of control over such self-generated content. Recipients of such material may distribute content further without the original producers' permission or the material may be obtained and distributed from children's hacked accounts, computers or other devices. The problem of free proliferation of user- or self-generated sexual content is increasingly recognized as widespread, with research findings suggesting that up to 88 per cent of self-generated, sexually explicit online content has been taken from its original location and uploaded elsewhere on the Internet without the original generator's permission.[126]

When content that meets the legal standard for child pornography is generated by minors without any adult involvement, coercion, or grooming, and is shared and transmitted solely between minors, child pornography possession and production offences may still technically be applicable, depending upon national ages of criminal responsibility. At the extreme, some content may even constitute evidence of statutory rape, depending upon the age of minors involved. Any criminal justice response to sexting acts may best focus on children who coerce the production of the material or who possess, use or distribute the material.[127] In addition, any criminal justice response must be considered as only one component of a wider social and educational response that supports teachers, parents, industry, and children to address often unequal and coercive sexual pressures, making them visible, available for discussion and open to resolution.[128]

Broadcasting of live sex abuse

As high speed Internet access, including mobile Internet, proliferates and becomes increasingly affordable, perpetrators can stream the sexual abuse of children in online live shows, making it harder to detect if it has not been captured or saved on a computer or mobile device. Through the use of

[117] *Ibid*., 2013.

[118] Quayle, E., et al. In Ainsaar, M., Lööf, L. (eds.). P. 14.

[119] A Thin Line, 2009. *2009 AP-MTV Digital Abuse Study. Executive Summary* Available at http://www.athinline.org/MTV-AP_Digital_Abuse_Study_.pdf.

[120] Ringrose, J., Gill, R., Livingstone, S., Harvey, L., 2012. *A Qualitative Study of Children, Young People and 'Sexting'. A Study Prepared for the NSPCC*. P. 6. Available at http://www.nspcc.org.uk/Inform/resourcesforprofessionals/sexualabuse/sexting-research-report_wdf89269.pdf.

[121] Lenhart, A., 2009. *Teens and Sexting: How and why minor teens are sending sexually suggestive nude or nearly nude images via text messaging. Pew Research Centre Report*. Available at http://pewresearch.org/assets/pdf/teens-and-sexting.pdf.

[122] See Leary, M., 2007. "Self-Produced Child Pornography: The Appropriate Societal Response to Juvenile Self-Sexual Exploitation", *Virginia Journal of Social Policy and the Law* 15:1-50; Leary, M. 2010. "Sexting or Self-Produced Child Pornography? The Dialogue Continues – Structured Prosecutorial Discretion within a Multidisciplinary Response". *Virginia Journal of Social Policy and the Law* 17:486-566.

[123] Some of the variation is due to variations in definitions (see Ringrose, J., Gill, R., Livingstone, S., Harvey, L., 2012. P. 6.)

[124] Leary, M., 2007.

[125] A Thin Line, 2009.

[126] IWF, 2012. Young people are warned they may lose control over their images and videos once they are uploaded online. Available at https://www.iwf.org.uk/about-iwf/news/post/334-young-people-are-warned-they-may-lose-control-over-their-images-and-videos-once-they-are-uploaded-online.

[127] See in general Leary, M., 2007; Leary, M., 2010.

[128] Ringrose, J., Gill, R., Livingstone, S., Harvey, L., 2012. P. 8.

"cyber-sex" dens, children can be sexually abused by an adult while images of the abuse are streamed live on the Internet, with access to the stream being commonly purchased via credit card. This form of child sexual abuse material requires only Internet connectivity, a computer with a built-in camera, a mobile phone or other mobile device with video functionality, or a detachable webcam. The live show format enables remote viewers to feel connected to the sexual activity, particularly as they can simulate active participation in the abuse by, for instance, directing the conduct of the people featured.[129] Live images of abuse may also be recorded for future distribution in order to generate maximum profit.

Victimization risk factors

Risk factors represent circumstances that may increase the likelihood of child victimization for certain offences. Such factors may be external, relating to the child's family and social environment, or concern characteristics or behaviour of the child victim himself or herself. Risk factors do not correspond to certainties, and are derived only retrospectively from observed associations between such factors and victimization outcomes across child cohorts. In particular, risk factors may be offset by protective factors that correspond to circumstances that decrease the likelihood of victimization, including through intervention in otherwise risky situations.

Gender and sexual orientation

Research indicates that girls account for the majority of victims of child abuse and exploitation, although boys are increasingly at risk as well.[130] In a sample of nearly 250,000 images of child sexual abuse material submitted to the Child Exploitation and Online Protection Centre in the United Kingdom between 2005 and 2009, four times as many images featured girls as compared to boys.[131] More recent figures from the IWF show that up to 76 per cent of sexual abuse images on the Internet featured girls in 2013, while 10 per cent featured boys and 9 per cent featured both genders.[132]

With respect to the commercial sexual abuse and exploitation of children, the International Labour Organization (ILO) estimates that 1.2 million children are trafficked per year and 1.8 million children are exploited annually in the global sex trade, of which about two-thirds are female. In cases of children abused and exploited in the travel and tourism industries, girls are again most frequently victimized.[133] Increasing attention is paid, however, to male victims of child sexual exploitation. The United States Department of State Trafficking in Persons Report of 2008, for example, identified male victims as a topic of special import. Noting that both ILO and UNICEF have found that male victims make up only two percent of documented child victims of commercial sexual exploitation, the report suggested that male victimization might be more widespread than reported, especially in light of the circumstance that boys may often feel reluctant to reveal their abuse because of a double stigma associated with suffering abuse and same-sex sexual relations.[134]

With respect to cyberenticement, up to 99 per cent of solicitations are made by men, mostly (43 per cent) youth or young adults, and are overwhelmingly (70 to 75 per cent) addressed to girls, with 14 to 17-year-olds being particularly at risk.[135]

With respect to user-generated content such as "sexting", girls may be disproportionately victimized. A 2012 study described the gender dynamics involved in sexting as follows:

> "Sexting is not a gender-neutral practice; it is shaped by the gender dynamics of the peer group in which, primarily, boys harass girls, and it is exacerbated by the gendered norms of popular culture, family and school that fail to recognise the problem or to support

[129] U.S. Department of State, 2007. P. 23; see also CEOP, 2013. Paragraphs 24, 33.

[130] See Cooper, S., Medical Analysis of Child Pornography. In S. Cooper et al. (eds.), 2005. *Medical, Social and Legal Aspects of Child Sexual Exploitation*. But see CEOP, 2013. Paragraph 29 (Observing a marked shift to fewer boy victims and more and younger girl victims in an analysis of an albeit small sample of recent offences in the United Kingdom).

[131] Quayle, E., Jones, T., 2011. "Sexualized Images of Children on the Internet", *Sexual Abuse: A Journal of Research and Treatment* 23:14.

[132] IWF, 2014. P. 6.

[133] ILO, 2002. *Every Child Counts. New Global Estimates on Child Labour*.

[134] U.S. Department of State, 2008. *Trafficking in Persons Report*. P. 9. Available at http://www.state.gov/documents/organization/105501.pdf.

[135] The Berkman Center for Internet & Society at Harvard University, 2008. *Enhancing Child Safety & Online Technologies: Final Report of the Internet Safety Technical Task Force to the Multi-State Working Group on Social Networking of State Attorneys General of the United States*. P. 20. Retrieved from http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/ISTTF_Final_Report.pdf.

girls. We found considerable evidence of an age-old double standard, by which sexually active boys are to be admired and 'rated', while sexually active girls are denigrated and despised as 'sluts'. This creates gender specific risks where girls are unable to openly speak about sexual activities and practices, while boys are at risk of peer exclusion if they do not brag about sexual experiences."[136]

Technology plays an important role in exacerbating this effect, with mobile phones and other devices, social networking sites, and other communication technologies facilitating the objectification of girls by allowing the creation, exchange, collection, ranking and display of images.[137]

Girls also suffer more frequently from cyberbullying. A survey conducted by Microsoft found that worldwide, 37 per cent of children aged 8-17 years had been subjected to a range of online activities such as mean or unfriendly treatment, being made fun of or teased, or being called mean names. Of that number, 55 per cent were girls.[138] Similarly, girls seem to suffer more from cyberbullying, with 37 per cent of those who had been bullied online in the past 12 months stating they had been very upset after the attack and 24 per cent reporting they had felt fairly upset, as opposed to 23 per cent respectively of male victims of bullying.[139]

Conversely, harm from exposure to inappropriate content most often affects boys. Because boys make up a larger percentage of video game players, they tend to see more of the violent and sometimes gendered content that commonly characterizes the online gaming environment. In other contexts, adolescent boys who seek out pornography with particular kinds of material in mind can find that searches retrieve more graphic and violent material than they expected. On the other hand, girls may be exposed to a higher proportion of harmful content in the context of child sexual abuse material and sexually explicit self-generated material sent by perpetrators during a grooming process.[140]

Youth identifying themselves as lesbian, gay, bisexual, or transgender may be more likely to receive online solicitations and can experience higher degrees of cyberbullying or harassment. In particular, boys who are gay or exploring their sexual orientation may be more liable to become involved in or to be victimized in Internet-initiated sex crimes than other children.[141] With respect to harassing conduct, a recent study in the United States found that more than 50 per cent of LGBT youth reported being subjected to cyberbullying.[142]

Prior abuse and family dysfunction

Prior abuse and family dysfunction also elevate the risk of victimization, particularly for commercial sexual exploitation of children. A study by UNICEF in the context of the Pacific region, suggests that commercial sexual abuse may be associated with prior abuse in a non-commercial context.[143] Half of the children in the study engaged in trafficking for the purposes of sexual exploitation reported previous sexual abuse.[144] A meta-review of 20 relevant studies concluded that the percentage of commercial sex trafficking victims who had previously been abused as children ranged from 33 per cent to 84 per cent.[145] Children who run away from or are "thrown

[136] NSPCC, 2012. Children, *Young People and 'Sexting'. Summary of Qualitative Study*. P. 12. Available at http://www.nspcc.org.uk/Inform/resourcesforprofessionals/sexualabuse/sexting-research-summary_wdf89270.pdf; see generally Ringrose, J., Gill, R., Livingstone, S., Harvey, L., 2012.

[137] NSPCC, 2012. P. 14.

[138] Cross-Tab Marketing Services & Telecommunications Research Group for Microsoft Corporation, 2012. *Online Bullying Among Youth 8-17 Years Old – Worldwide. Executive Summary*. Available at http://www.microsoft.com/security/resources/research.aspx#onlinebullying.

[139] Staksrud, E., 2011.

[140] Ybarra, M., Mitchell, K., 2005. "Exposure to Internet Pornography among Children and Adolescents: A National Survey", *CyberPsychology and Behaviour* 8:473-485; Mitchell, K., Finkelhor, D., Wolak, J., 2003; Wolak, J., Mitchell, K., Finkelhor, D., 2007; OECD, 2011. The Protection of Children Online. Risks Faced by Children Online and Policies to Protect them. Available at http://www.oecd-ilibrary.org/science-and-technology/the-protection-of-children-online_5kgcjf71pl28-en.

[141] Online "Predators" and Their Victims: Myths, Realities, and Implications for Prevention and Treatment, Janis Wolak, PhD, David Finkelhor, PhD and Kimberley J. Mitchell, PhD Crimes Against Children Center at the University of New Hampshire and Michelle L. Ybarra, PhD, "Internet Solutions for Kids, Inc.", *American Psychologist*, Vol. 63, No.2. Available at http://www.apa.org/pubs/journals/releases/amp-632111.pdf

[142] Blumenfeld, W. J., Cooper, R. M., 2010. "LGBT and Allied Youth Responses to Cyberbullying: Policy Implications", *International Journal of Critical Pedagogy* 3:114-133.

[143] UNICEF, 2006. *Child Sexual Abuse and Commercial Sexual Exploitation of Children in the Pacific Region*. Available at http://www.unicef.org/eapro/Pacific_CSEC_report.pdf.

[144] *Ibid.*

[145] J. Raphael, 2004. *Listening to Olivia: Violence, Poverty, and Prostitution*.

away,"[146] by their families, are twice as vulnerable to exploitation once they become homeless.[147] Runaway children quickly find themselves deprived of food, shelter and security[148] and some resort to "survival sex" as a means of meeting those basic needs.[149] Such forays into commercial sex can have the effect of grooming children for longer-term commercial sexual exploitation. In short, children who are already isolated, starving, sleep-deprived, and sometimes resigned to sexual exploitation, make easy targets for offenders.

Children who suffer from prior abuse may struggle with damage to their self-esteem or a sense of stigma[150] that offenders can exploit. Research undertaken in the Netherlands suggests that personal factors, such as low self-esteem or family dysfunction, heighten a child's vulnerability to trafficking for purposes of sexual exploitation.[151]

Such children may not easily be reached by law enforcement or social welfare or protection services. Street children may eschew potential sources of support because they fear being returned to abusive home situations. They may also fear law enforcement and criminal justice services as a result of involvement in offences such as stealing and squatting in order to meet survival needs.

Poverty and migration

Direct research on the relationship between poverty and migration patterns, and ICT-facilitated abuse and exploitation of children, is limited. To the extent, however, that poverty and migration represent risk factors for abuse and exploitation of children in general,[152] broad associations may also exist in respect of such conduct that also involves ICTs. For example, a family or community member might use traditional offline means to recruit a child for work in another country under the pretence of offering employment such as domestic work. Once in the destination country, however, the child may be forced to engage in commercial sex or in the production of child sexual abuse material.[153] One study of children trafficked for the purposes of sexual exploitation in the United States, Canada, and Mexico identified poverty as the most consistent common trait of victims.[154]

Age

Very young children are increasingly victimized in child sexual abuse material and child sex trafficking. Recent figures from the Internet Watch Foundation suggest that as many as 81 per cent of victims in known child abuse images are ten and under, and three per cent are two years of age or younger. This figure is up from 74 per cent in 2011.[155] Another recent study found that 83 per cent of child sexual abuse material-consumers possessed videos or images displaying prepubescent children. Of these, over 80 per cent owned material involving children between the ages of six and 12 years, and around 40 per cent had images of children between the ages of three and five. Alarmingly, 19 per cent of child sexual abuse material-possessors had images of babies and infants under the age of three.[156]

Sexual exploiters of children may also engage very young children in commercial sex. The average age of sex tourism victims is estimated to be 14 years, although victimization of children as young as five years old is becoming increasingly common.[157] Commercial sexual exploiters of children have

[146] The term "throwaways" or "throwaway children" refers to children whose guardians have formally or informally ejected them from their homes and from familial support (Estes,.R. J., Weiner, N. A., 2002. *The Commercial Sexual Exploitation of Children in the U.S., Canada, and Mexico*. University of Pennsylvania National Institute of Justice Research Publications. Pp. 110–111. Available at http://www.hawaii.edu/hivandaids/Commercial%20Sexual%20Exploitation%20of%20Children%20in%20the%20US,%20Canada%20and%20Mexico.pdf).

[147] ECPAT International, 2008. *Combatting Child Sex Tourism, Questions and Answers*. Avilable at http://www.ecpat.net/ei/Publications/CST/CST_FAQ_ENG.pdf.

[148] *Ibid*.

[149] *Ibid*.

[150] UNICEF, 2006.

[151] Research in South Eastern Europe similarly found that poverty, alcoholism, family dysfunction, drug abuse, sexual abuse and domestic violence combine to escalate children's risk of exploitation (UNDP. 2005. *Trafficking in Human Beings in South Eastern Europe: 2004 - Focus on Prevention in: Albania, Bosnia and Herzegovina, Bulgaria, Croatia, the former Yugoslav Republic of Macedonia, Moldova, Romania, Serbia and Montenegro, the United Nnations Administered Province of Kosovo*; see also UNICEF, 2007. *Child Trafficking in Europe: A Broad Vision to Put Children First*.

[152] Bartlett, S. 2009. *Environments of Poverty and What they Mean for Child Protection*. Save the Children, Sweden.

[153] Trinidad, A.C. 2005. P. 67.

[154] Estes, R. J., Weiner, N. A., 2002. Pp. 41-42.

[155] IWF, 2014. P. 11.

[156] NCMEC, 2005. *Child Pornography Possessors Arrested in Internet-Related Crimes: Findings for the National Juvenile Online Victimization Study*. Pp. vii, 4.

[157] World Vision "Child Sex Tourism Prevention" 2014 http://www.worldvision.org/worldvision/pr.nsf/stable/child_sex_tourism_background. (Noting that children are prostituted in virtually every country around the world. Currently, an estimated two million children worldwide - some as young as 5 years old - are enslaved in the commercial sex trade. Many of these children are forced, coerced or tricked into prostitution)

capitalized on the growing demand for young children by recruiting increasingly younger victims.[158]

Adolescents face the highest risk of cyberenticement, exposure to harmful material, and cyberbullying, particularly since they may be more prone than younger children to engage more readily in communications with strangers.[159] Adolescents are also more likely to post suggestive or indecent pictures of themselves in public and semi-public online forums, despite not necessarily having the necessary skills to recognize and disengage from dangerous situations.[160]

Studies show that cyberbullying also peaks during adolescence, at around 13 to 14 years of age,[161] with the vast majority of bullying victims aged between 12 and 17 years. The age range for cyberbullying victims correlates with that for offline bullying. This is not surprising, given that many instances of cyberbullying are ancillary to offline bullying. For instance, some bullies may target children at school and then continue to harass their victim out of school time, through online connections.[162]

Risky online behaviour and inattention to online safety and privacy

The extent to which children engage in risky online behaviour and neglect privacy and safety measures is one key factor that affects the degree of exploitation encountered. Children who engage in risky behaviour, both on- and offline, face a higher risk of exploitation. The 2009 European Union Kids Online study found that half of young Internet users made personal information available to strangers, 40 per cent viewed pornographic content online, 30 per cent viewed violent or hateful content of some sort, while ten per cent agreed to in-person contact with an online friend.[163] In a 2012 survey, 44 per cent of teens surveyed admitted they have looked at something online of which their parents would not approve[164] and, according to a 2011 survey, 42 per cent of teens admitted they had cleared their browsing history after using the Internet.[165]

Regarding cyberenticement, solicitation or grooming, young people who engage in risky or aggressive online behaviour, such as making rude comments in online forums, visiting pornographic websites or opening material they receive from strangers through peer-to-peer-networking sites, tend to receive more explicit solicitations.[166] Levels of risk increase with children's willingness to discuss sexual topics with strangers online.[167] One recent study noted that children who engaged in four or more risky types of online behaviour were much more likely than others to report receiving online sexual solicitations. Although some technologies can be more easily utilized for purposes of solicitation than others, solicitation risk levels appear to be more clearly associated with psychosocial profile and risky behaviour, than with any particular technological platform.[168]

Closely related to the topic of risky online behaviour, is young peoples' inattention to online safety and privacy. Children who are not sufficiently attentive of online safety precautions may be at much greater risk of cyberenticement and cyberstalking. Whereas perpetrators might initially target a wide array of children, they will be most successful in amassing information about children who carelessly share personal information and pictures, especially certain kinds of information, such as age and geographic location. Children may reveal their age, for instance, by publishing dates of birth or by posting pictures, commenting on age-specific subjects such as movies or video games, or by mentioning their school. Along similar lines, offenders may gain real-time information about physical location where a child uses online applications

[158] Shared Hope International "FAQs about child sex trafficking" 2014 http://sharedhope.org/learn/faqs/

[159] The Berkman Center for Internet & Society at Harvard University, 2008. Pp. 19-20, 39-40.

[160] Choo, K. R., 2009. P. 7 (Noting that children are still learning how to communicate effectively so they are less likely to be as socially skilled as adults (internal citations omitted).

[161] The Berkman Center for Internet & Society at Harvard University, 2008. P. 11.

[162] Lenhart, A., 2007. *Cyberbullying and Online Teens*. Pew Internet and American Life Project. Available at http://www.pewInternet.org/2007/06/27/cyberbullying/.

[163] Livingstone, S., Haddon, L., 2009. P. 16.

[164] Cox Communications, "Tween Internet safety survey," June 2012. http://ww2.cox.com/wcm/en/aboutus/datasheet/takecharge/tween-Internet-safety-survey.pdf (accessed Dec. 27, 2012).

[165] GFI Software, 2011. 2011 parent-teen Internet safety report. P. 7. Available at http://www.gfi.com/documents/GFI%20_2011_parent_teen_Internet_safety_report_june.pdf.

[166] The Berkman Center for Internet & Society at Harvard University, 2008; see also Wolak J., Finkelhor, D., Mitchell, K.J., Ybarra, M.L., 2008. "Online 'Predators' and Their Victims: Myths, Realities, and Implications for Prevention and Treatment", *American Psychologist* 63:118. Available at http://www.apa.org/pubs/journals/releases/amp-632111.pdf.

[167] The Berkman Center for Internet & Society at Harvard University, 2008. P. 20.

[168] The Berkman Center for Internet & Society at Harvard University, 2008.

to "check-in" to places and track their current location. Youth who do not follow online safety precautions may also tend to receive more harmful content than more prudent peers. Similarly, children with publicly available social media profiles are likely to receive more unsolicited messages from strangers via Internet messaging, e-mail and text and experience higher levels of cyberharassment and bullying than those with private profiles.[169] In addition to social profiles that are inextricably linked with real world identity, the Internet also offers children the opportunity to create a separate identity, through which they can be whomever they wish and perhaps take risks that they would never take offline.

One relatively new channel of access to victims has arisen through the phenomenon of connected, or online, gaming. Online gaming can be adrenaline-charged with depictions of violence, and is designed to engage players for sustained periods of gaming time. Many gamers become attached to points, "assets," or other markers of gaming success, leading even to cases where children have committed suicide after losing such indicators.[170] Some users, including children, become obsessed with online gaming and begin to prefer their virtual life to their slow-paced and less easily controlled reality. As a result, youthful gamers are especially vulnerable to offenders who try to engage them in relationships in the virtual setting. Like other online forums, online gaming communications do not offer the real-world social cues that would normally alert youth to inappropriate advances. Further, online gamers can manipulate their social status by surrounding themselves with virtual friends. Offenders may use this phenomenon to their advantage by offering to help children with their gaming performance in exchange for online or offline sexual encounters, or by initiating a relationship for the purposes of committing such acts in the future.

Social isolation

Social isolation can have negative repercussions on children's online behaviour, as well as on their propensity to seek help when problems arise. Research on socially isolated young people suggests that they may face an increased risk of certain forms of exploitation, as well as bullying.[171] Rejected or neglected by real-life friends, children who feel isolated may turn to online friends as a substitute. Where social networking sites count and report the number of friends that each user has amassed, children may be motivated to add online friends, even if they are effectively strangers.[172] Children may publicly share information with groups of online friends, including potential perpetrators. In some cases, this may include inappropriate or sexually explicit material, with a view to gaining acceptance and attention.

Profile of offenders

As with descriptions of risk factors for victimization, information on offender profiles corresponds only to broad results from studies of cohorts of identified offenders. Offender "profiles" may contain many descriptor elements, including age, sex, socioeconomic background, nationality, motivation, and past victimization. While factors such as age and social status, offending patterns, and links with "offline" offending, may be used to generate a broad picture of offender characteristics,[173] it is also clear that there is no single "typical" offender. This section reviews relationships between offending behaviour and motivation, gender, age, and technological awareness, as well as the involvement of organized criminal groups in ICT-facilitated abuse and exploitation of children.

General profile and motivations of offenders

Motives for committing child sex abuse and viewing child sexual abuse material vary. Research suggests that the desire for sexual gratification serves as the driving motivation for most child sexual abuse material consumers. While many "lone" individuals possess and view such material, some offenders may also enjoy the camaraderie they experience through online communities.[174] Personality studies of child sexual abuse material consumers indicate a "rejecting and submissive interpersonal style, which preclude[s] effective

[169] Lenhart, A., et al., 2011. *Teens, Kindness and Cruelty on Social Network Sites*. Pew Internet & American Life Project. Pp. 61-64. Available at http://pewInternet.org/Reports/2011/Teens-and-social-media/Part-3/Introduction.aspx.

[170] Bose, A., 2013.

[171] Schwartz, D., Proctor, L. J., Chien, D. H. The Aggressive Victim of Bullying: Emotional and Behavioural Dysregulation as a Pathway to Victimization by Peers. In Juvonen, J., Graham, S. (eds.), 2001. *Peer Harassment in School: The Plight of the Vulnerable and Victimized*. Pp. 47-174.

[172] See Choo, K. R., 2009. Pp. 7-11.

[173] UNODC, 2013. *Comprehensive Study on Cybercrime*. P. 43-44.

[174] Quayle, E., Taylor, M., 2002. "Child pornography and the Internet: perpetuating a cycle of abuse", *Deviant Behaviour: An Interdisciplinary Journal*, 23:331-361.

interaction with others".[175] Some child sexual abuse material offenders may have low emotional stability, and/or exhibit relatively high levels of depression.[176] The concept of Internet addiction disorder[177]—understood as an overuse of the Internet that is so excessive as to interfere with the ability to function and participate in daily life—may also be applicable in the case of some child sexual abuse material offenders.[178] Offenders may use the concept of addiction to ease their sense of guilt about the offending behaviour.

Research also characterizes a dichotomy of possible social motivations among child sexual abuse material offenders. One set of offenders consists of socially isolated persons with intimacy deficits who try to make up for emotional and sexual needs through online sexual activity. Another type of offenders consists of those who use the Internet to avoid real-world emotions and for whom interacting with child sexual abuse material serves as a soothing strategy when confronted with emotional distress.[179] Other related typologies differentiate between "morally indiscriminant" offenders, whose child sexual abuse material-related offences constitute only part of their engagement in a broad variety of illegal conduct, and "profiteers" who seek to generate money from the lucrative child sexual abuse material market. Although the latter may feel morally ambivalent about child sexual abuse material or even object to the exploitation per se, their interest in profit overrides their misgivings. Alternatively, commercial providers may have an interest in child sexual abuse material themselves, and may seek to add to their own contacts and collections of illicit material through commercial activities.[180]

Another important typology ranks offenders by the degree of seriousness of their conduct. One measure of seriousness is the level of in-person contact with victims involved, which ranks contact offences as more serious than non-contact offences. Another point of reference is the degree to which offenders protect access to their child sexual abuse material collections for the purposes of evading detection by law enforcement. In this respect, levels of protection of child sexual abuse material may serve as a measurement of perpetrator levels of involvement in child exploitation.[181]

Research also considers offenders' motivation to commit cyberenticement or grooming offences. A recent European Union report classified offenders into three groups according to their motivations. The first category consists of "intimacy seekers", who consider their relationships with children to be both romantic and consensual and tend to refrain from collecting large caches of child sexual abuse material, instead focusing their time and energy on pushing for in-person encounters with children. The second category in this typology consists of "adaptable offenders", believing that their victims are precociously sexually mature, so that they are genuinely capable of consenting to the relationship. Thirdly, "hypersexual offenders" constitute the most serious category and possess vast collections of pornographic material.[182]

Cyberenticers are driven by their desire to engage in sexual acts with children or at least by a wish to fuel their fantasies about such unions. They often create sophisticated online personas for the express purpose of enticing children to produce self-created pornographic content through webcams. They may typically try to seduce multiple children at once, while wasting little time in escalating online conversations to a sexual tone. Cyberenticers also typically join groups of and communicate with other offenders for both social affirmation and tactical advice. The most frequent aggressive online sexual solicitations involve asking to meet a child in person (seven per cent of cases), calling a young person on the telephone (34 per cent of cases), coming to the home of the young person (18 percent of cases), giving a young person money, gifts or other items (12 per cent of cases), sending offline mail to a young person (nine per cent of cases), and buying travel tickets for a young person (three per cent of cases).[183]

People who transmit harmful content to children have varied motivations. Many simply gain satisfaction from the idea of causing harm to children. For instance, children using peer-to-peer file-sharing programs may open pornographic content because the files have been mislabeled. Along similar

[175] Laulik, S., Allam, J., Sheridan, L., 2007. "An investigation into maladaptive personality functioning in Internet sex offenders", *Psychology, Crime & Law* 13:531.

[176] See *ibid*.

[177] See e.g. Young, K. S., 1998. "Internet Addiction: The Emergence of a New Clinical Disorder", *CyberPsychology and Behaviour* 1237-244; Grundner, T. M., 2000. *The Skinner Box Effect: Sexual Addiction and Online Pornography*; Greenfield, D., 2010. *Clinical Treatment of Internet and Digitally-enabled Compulsive Behaviour.*

[178] Byun, S., et al., 2009. "Internet Addiction", *CyberPsychology & Behaviour* 12: 203–204.

[179] Quayle, E., Taylor, M., 2002.

[180] Beech A., et al., 2008. P. 225.

[181] *Ibid*. Pp. 224-225.

[182] Webster, S., et al., 2012. *European Online Grooming Project. Final Report*. Pp. 13-14.

[183] Wolak, J., et al., 2006. *Online Victimization of Youth Five Years Later*. Available at http://www.missingkids.com/en_US/publications/NC167.pdf.

lines, perpetrators may set up websites with explicit content including pornography, and select URLs (uniform resource locators) that contain small or common misspellings of the names websites intended for use by children. Conversely, transmission of harmful material to children may be profit-motivated. For example, professional spam operations that send out millions of e-mails advertising pornography or other explicit content may simply not care about the harmful consequences of such material on children.[184]

Results vary widely on the link between non-contact child sexual abuse material offenders and contact abusers.[185] Studies suggest, however, that at least some offenders commit both contact and non-contact offences.[186] While the degree and details of such overlap remains the subject of significant debate,[187] researchers have documented substantial overlap among criminal convict populations.[188] Specifically, in one long-term study of offenders convicted for non-contact child sexual abuse material crimes, 85 per cent eventually disclosed that they also had committed undetected contact abuse.[189] Other research suggests that investigating cases of child sexual abuse material possession often leads to arrests for child sexual abuse, corroborating the findings of self-disclosure research.[190]

Conversely, many perpetrators arrested for contact offences are found to possess significant collections of child sexual abuse material.[191] Research also indicates that contact offenders have longer criminal records,[192] more often have a history of child sexual abuse, and tend to use emotionally charged coping strategies when under stress.[193] While contact offenders report high levels of previous sexual abuse, non-contact offenders report a more complex history of childhood problems associated with early childhood sexual experience and sequentially abusive adult sexual experience.[194] One recent review concluded, for example, that: "[i]t is evident that there are differences between Internet and contact offenders related to demographic characteristics such as age, level of education, and measure of intelligence as well as psychological variables".[195]

Most possessors of child sexual abuse material are preferential child sex offenders, or paedophiles,[196] who use the material to nurture their sexual fantasies about children or as proof of their conquests in offender communities.[197] Preferential child sex offence conduct is also linked to the commercial sexual abuse and exploitation of children in the travel and tourism industries.[198]

In a different category of offenders, families may exploit their own or other local children by producing sexual abuse material solely for profit. In some cases, a child may be made to stand naked in front of a webcam, and the family member may not even consider such behaviour to constitute sexual abuse or harm to the child.[199]

---

[184] See, for example, OECD, 2011; House of Commons Culture, Media and Sport Committee, 2008. *Harmful content on the Internet and in video games. Tenth Report of Session 2007–08*.

[185] See e.g. Bourke M. L., Hernández. A., 2009. "The Butner Study Redux", *Journal of Family Violence* 24:183-191.

[186] See, for example, Beech, et al., 2008.

[187] See generally Neutze, J., et. al, 2010. "Predictors of child porngraphy offences and child sexual abuse in a community sample of paedophiles and hebophiles", *Sexual Abuse: A Journal of Research and Treatment* 22(4):3-24.

[188] Seto, M., 2010. "Child Pornography Use and Internet Solicitation in the Diagnosis of Pedophilia", *Archive of Sexual Behaviour* 39:591–593.

[189] Bourke M. L., Hernandez, A., 2009.

[190] Wolak J., Finkelhor, D., Mitchell, K.J., Ybarra, M.L., 2008.

[191] United Nations Human Rights Council, 2009. *Report of the Special Rapporteur on the Sale of Children, Child Prostitution and Child sex abuse material* [A/HRC/12/23]. Paragraph 42.

[192] Caution must be exercised in interpreting conviction data. Overall reporting rates for child abuse are estimated at approximately one-third for girls and one quarter for boys. Only 5 per cent of victims in a 2011 United Kingdom study reported making a formal complaint to police. From this small percentage of reported victimization, only 7 per cent result in criminal convictions. Persons convicted thus correspond to a small, and not-necessarily representative sample of the whole population of sexual abusers; Joseph Sullivan, 2013. Commentary at the Informal Expert Group Meeting on the Effects of Information and Communication Technologies on the Abuse and Exploitation of Children. Vienna. September 23, 2013 through September 26, 2013.

[193] Howitt, D., Sheldon, K., 2007. Pp. 139-172

[194] Howitt, D., Sheldon, K., 2007. Pp. 123-160.

[195] Quayle, E., Sinclair, R., An introduction to the problem. In Quayle, E., Ribisl, K. (eds.), 2012. *Understanding and Preventing Online Sexual Exploitation of Children*. P. 7.

[196] Seto, M. C., 2010.

[197] The Berkman Center for Internet & Society at Harvard University, 2008. P. 37.

[198] ECPAT. *End Child Prostitution, Child Pornography & Trafficking of Children for Sexual Purposes*. Available at: http://www.ecpat.net/faqs#child-sex-tourism.

[199] See e.g. CEOP, 2013. Paragraph 24.

Gender

While both men and women may participate in child exploitation, male perpetrators tend to constitute the majority of offenders with regard to child sexual abuse material-related conduct, cyberenticement, and cyberstalking. Conversely, certain forms of exploitation including trafficking and cyberbullying can have a high prevalence of female perpetrators.

Research suggests that offenders in child sexual abuse material-related conduct are most commonly adult men, operating alone.[200] A recent study on child sexual abuse material-consumption found, however, that 5.5 per cent of the women sampled had also engaged with such material.[201] Some women are also reported to be among the clients of the commercial sex trade, including international sex tourism. Because most research on female sexual abusers has been conducted before the widespread nature of ICTs, however, little is known about current patterns of abuse.[202]

On the other hand, both men and women commit commercial sexual exploitation of children, though their roles tend to differ depending on the concrete conduct involved. Male commercial sexual exploiters of children tend to be more involved in the "practical" aspects of child abuse and exploitation, as they are usually better able to exert physical force to abduct child victims and to enforce obedience through violence. Men may also forge feigned romantic relationships with young female victims as a means of recruiting them into exploitation. Women, on the other hand, may more commonly engage in the business end of operating commercial sexual exploitation of children enterprises, as well as, in some cases, recruitment of victims through a process of "friendship" and trust-gaining.

The vast majority of cyberenticement offenders are male. Though the most common dynamic involves an adult male enticing or soliciting a female victim, victims may be both male and female. Generally, research has concluded that women are seldom the primary actors in child sex abuse, including cyberenticement, and that those who do participate in such abuse may be motivated by a desire to please male co-actors.[203] It is possible, in some contexts, that a low law enforcement priority on detecting and investigating female offending conduct, leads to an underrepresentation of female offending in public perception and crime statistics.[204]

Harassing behaviour is more gender-neutral, both on- and offline. Men and women may equally engage in offline stalking and in cyberstalking, and can even be just as likely to resort to violence subsequent to harassing behaviour. Victims, especially male victims, of harassment perpetrated by female offenders may be less likely to report victimization, either because of embarrassment or because they do not consider that the harassment constitutes any serious threat to their safety. However, male stalkers are shown to be more likely than women stalkers to ignore rejection by a victim.[205]

Gender similarly does not constitute a prominent feature in the profile of cyberbullies.[206] However, modes of bullying may differ between male and female perpetrators. Whereas it is more common for girls to speak negatively about others, boys are more likely to post negative pictures or videos.[207]

Age

In describing the age range of offenders, it is important to note that research over the last decade has centered on offenders who reached the age of majority before the widespread accessibility of child sexual abuse material on the Internet. As a result, information gaps exist with respect to the impact that

[200] Finkelhor, D., Ormrod, R. K., 2004. "Child Pornography: Patterns from NIBRS", *U.S. Department of Justice Juvenile Justice Bulletin*; see also Aebi M., et al., 2012. Offender Types and Criminality Dimensions in Male Juveniles Convicted of Sexual Offences. *Sexual Abuse*. 24: 282.

[201] Seigfried-Spellar K. C., Rogers, M. K., 2010. "Low Neuroticism and High Hedonistic Traits for Female Internet Child Pornography Consumers", *Cyberpsychology, Behaviour, and Social Networking* 13:634.

[202] See Grayson, A., De Luca, R. V., 1999. "Female Perpetrators Of Child Sexual Abuse: A Review Of The Clinical And Empirical Literature", *Aggression and Violent Behaviour*, 4:93–106.

[203] Brayley, H., Cockbain, E., 2012. *Group-Based Child Sexual Exploitation*. Available at http://www.ucl.ac.uk/jdibrief/crime/child-sex-exploitation.

[204] See for example, Hendriks J., Bijleveld, C.C.J.H., 2006. Female adolescent sex offenders—An exploratory study. *Journal of Sexual Aggression* 12:33; Bexson, 2011. "'The Ultimate Betrayal'. Female Child Sex Offenders", *Internet Journal of Criminology* 2011:1-25; see also generally Denov, M. S., 2004. *Perspectives on female sex offending: A culture of denial*; van der Put, C., van Vugt, E., Stams, G. J., Hendriks, J., 2012. "Psychosocial and Developmental Characteristics of Female Adolescents Who Have Committed Sexual Offences", *Sexual Abuse: A Journal of Research and Treatment* 25:41-68; van der Put, C. E., 2013. "The prevalence of risk factors for general recidivism in female adolescent sexual offenders: A comparison of three subgroups", *Child Abuse & Neglect* 37:691-697.

[205] University of Houston, Stalking and Cyberstalking, Available at http://www.uh.edu/wrc/safety-and-violence-prevention/stalking%20/index.php.

[206] Görzig, A., 2011. *Who bullies and who is bullied online?: a study of 9-16 year old Internet users in 25 European countries*. EU Kids Online network. P. 5.

[207] Cyberbullying Research Center, *Research in Review* (2004-2010). Available at http://www.cyberbullying.us/research.php.

current levels of access have on offending profiles, including age. Research in the United States, for instance, on convicted child sexual abuse material offenders between the years 2000 and 2005 found that a higher proportion of adult offenders were ages 18 to 25 than in previous research.[208]

Nonetheless, with this effect in mind, analysis of data on 103 male subjects who had been arrested for using peer-to-peer technology to download or transmit child sexual abuse material indicates that the average age of offenders was 41, with a range of 15 to 73 years of age.[209] Married or cohabiting offenders tended to be older (age 50 on average) than those who were single (age 35 on average).[210]

Research on adolescent child sexual exploiters and abusers is becoming increasingly important. In a study of male adolescent sexual abuse conduct, researchers found that male offenders exhibited relatively high levels of drug and alcohol abuse, behaviour problems, and histories of delinquency. Research also suggests that they may less commonly have histories of sexual abuse victimization than their older counterparts. Female adolescent sexual abusers are thought to represent approximately five to ten per cent of all juvenile abusers.[211] Alarmingly however, female youth perpetrators tend to choose younger victims and to be more often involved in incidents involving multiple victims.[212]

Regarding cyberbullying, research suggests that the prime age for such aggressive behaviour is approximately 10 to 13 years.[213] Though less common, adults are also known to engage in cyberbullying of children.[214]

Other demographic characteristics

Research on other demographic characteristics has focused primarily on child sexual abuse material offenders. Perpetrator studies in North America suggest that child sexual abuse material offenders are mostly white and reasonably well educated.[215] Research on the marital status of child sexual abuse material offenders finds that a large portion of offenders—approximately 45 per cent—is single, another 28 per cent is married, and the remaining 27 per cent is divorced or separated.[216] The fact that child sexual abuse material offenders generally have comparatively high levels of education may correlate to offenders' comfort with and sophistication in the use of technology.[217]

Studies also indicate a possible association between contact offenders and experience of childhood emotional, physical or sexual abuse, as well as insecure parental attachments.[218] In one recent study, researchers concluded that both online and offline abusers are more likely to have themselves

[208] Wolak, J., Finkelhor, D., Mitchell, K., 2011. P. 28.

[209] UNODC, 2013. P. 43-44.

[210] *Ibid.*

[211] See e.g. Finkelhor, D., Ormrod, R., Chaffin, M. 2009. "Juveniles who commit sex offences against minors", *U.S. Department of Justice Juvenile Justice Bulletin*; Lane, S., Lobanov-Rostovsky, C., Special populations. In Ryan, G., Lane, S. (eds.), 1997. *Juvenile sexual offending*. Pp. 322–359; see generally van der Put, C. E., 2013.

[212] Van der Put, C. E., 2013. P. 691.

[213] Wade, A., Beran, T., 2011. "Cyberbullying: The New Era of Bullying", *Canadian Journal of School Psychology* 26: 44-61.

[214] In a 2006 United States case [*United States v. Drew*, 259 F.R.D. 449 (C.D. Cal. 2009)], the mother of a 13-year-old girl cyberbullied her daughter's classmate, resulting in the suicide of the child victim. The mother assumed the identity of a teen boy on a social networking site and then (virtually) courted the victim. The perpetrator suddenly then changed the tone of the communication and began tormenting the victim, even suggesting that the world would be a better place without her. Social network members has contributed to the bullying by posting derogatory comments. The victim replied that, "you're the kind of a boy that a girl would kill herself over", and then committed suicide. Charged with multiple counts of computer fraud, the perpetrator was only convicted of a single minor offence which was subsequently set aside on a motion for acquittal.

[215] Wortley, R., Smallbone, S., 2006. *Situational Prevention of Child Sexual Abuse*.

[216] Finkelhor, D., Mitchell, K.J., Wolak, J. 2005. Online Victimization: What Youth Tell Us. In Cooper, S.W., et al. (eds.), 2005. *Medical, Legal, and Social Science Aspects of Child Sexual Exploitation: A Comprehensive Review of Pornography*, Prostitution, and Internet Crimes. Pp. 437-467.

[217] *Ibid.*

[218] Craissati, J., McClurg, G., Browne, K., 2002. "The Parental Bonding Experiences of Sex Offenders: A Comparison Between Child Molesters and Rapists", *Child Abuse and Neglect* 26:909-921; Simons, D. A., Wurtele, S., Durham, R., 2008. "Developmental experiences of child sexual abusers and rapists", *Child Abuse and Neglect* 32:549-560.

experienced physical and sexual abuse than the general population.[219]

Research on offline sexual abuse is also important in understanding cyberenticement.[220] In research on juvenile sex abusers, exposure to intra-family violence appears to have important predictive value. Children who witness and experience violence including domestic violence seem to be at a particularly high risk of engaging in sexual abuse conduct in the future. It is possible that these "experiences of physical violence and the breaching of personal boundaries by assault may in some way give permission for the young person to go on to inflict sexual violence on another child".[221]

Studies on bullying in general demonstrate a cluster of behavioural problems in bullies, including aggression. A 2011 comparison of traditional and online bullies found that people who bully offline tend to resort to cyberbullying in order to amplify the impact on their victims.[222] Research indicates that cyber-bullies exhibit poor psychosocial skills that result in evident problems at school and other behavioural deficits, which may also at least in part explain the dynamics by which victims become aggressors.[223] Poor social functioning results in bullying especially when more vulnerable targets are encountered. Offenders may also tend to see aggression as an acceptable solution for problems and be more likely to use drugs and alcohol.[224] Those who suffer from cyberbullying and also engage in bullying others are shown to be the heaviest substance abusers.[225] Likewise, victims of solicitation are, on average, twice as likely to report substance use.[226]

[219] Quayle, E., Sinclair, R. In Quayle, E., Ribisl, K. (eds.), 2012. P. 7.

[220] Wolak, J., 2013. Commentary at the Informal Expert Group Meeting on the Effects of Information and Communication Technologies on the Abuse and Exploitation of Children. Vienna. September 23, 2013 through September 26, 2013.

[221] Vizard, E., 2013. "Practitioner Review: The victims and juvenile perpetrators of child sexual abuse –assessment and intervention", *Journal of Child Psychology and Psychiatry* 54:507.

[222] Sontag, L. M., et al., 2011. "Traditional and Cyber Aggressors and Victims: A Comparison of Psychosocial Characteristics", *Journal of Youth and Adolescence* 40:392-404.

[223] See e.g. Görzig, A., 2011.

[224] The Berkman Center for Internet & Society at Harvard University, 2008. P. 28.

[225] See The Berkman Center for Internet & Society at Harvard University, 2008. P. 42-43.

[226] Mitchell, K. J., Ybarra, M., Finkelhor, D., 2007. "The Relative Importance of Online Victimization in Understanding Depression, Delinquency, and Substance Use", *Child Maltreatment* 12: 320.

Technological sophistication

One typology of child sexual abuse material offenders is based on their level of technical expertise. Here, the least aggressive offenders are "simple viewers, who are primarily driven by curiosity and rarely download, save or trade child sexual abuse material with others." Next on the continuum are "open traders", motivated by the desire to add to their collections of child sexual abuse material. Open traders use tight security, though not as extreme as "closed traders", who are more committed to guaranteeing their continued access to such material. Closed traders may try to eliminate undercover law enforcement agents by insisting that new traders in a community site upload child sexual abuse material before they are allowed full access. Closed traders tend to form close bonds with other child sexual abuse material offenders with whom they engage in online forums and other virtual communities. Finally, the "experts" make up the most committed set of child sexual abuse material offenders in this typology. These offenders tend to have long histories of active engagement in child sexual abuse material possession and trading and are highly skilled and diligent about security measures in order to evade detection.[227]

As concerns other offences, cyberstalkers are typically highly sophisticated technical users, deploying the same tactics that criminals use to commit other cybercrimes, including identity theft or hacking. These techniques enable them to obtain private information about their targets, such as home addresses and dates of birth. Cyberstalkers develop expertise on using such information together with other online sources to accumulate yet more information about their victims. Research on cyberbullying reveals associations between cyberbullying, technological proficiency and the amount of time spent online, suggesting that bullies may also have the potential to employ more aggressive stalking techniques, through an ability to make maximum use of online material in the targeting of others.[228]

[227] Aiken, M., Moran M., Berry, M., 2011. *Child abuse material and the Internet: Cyberpsychology of online child related sex offending*. Paper presented at the 29th Meeting of the INTERPOL Specialist Group on Crimes against Children Lyons, France, 5-7 September 2011. Available at http://goo.gl/UQSZ52; see also, D. Greenfield, *Clinical Treatment of Internet and Digitally-enabled Compulsive Behaviour* (2010). Available at http://www.virtual-addiction.com/pages/documents/ ClinicalTreatmentofInternet-SpainChapter_000.pdf.

[228] Wade, A., Beran, T., 2011.

Groups of offenders

The majority of child sexual abuse material is exchanged via non-commercial channels, including public peer-to-peer platforms, as well as Tor, or the dark web.[229] A large number of loose online groups of offenders exist around such platforms. Such groups may trade in specific forms of child abuse material, such as specific types of children based on gender or race. Others groups may enable users to share tactics on committing child sexual abuse material-related offences. Still others may specialize in providing advice to those in search of victims for contact abuse. Many groups serve all of these purposes simultaneously. While some commercial activity may occur, such groups tend to be primarily focused on facilitation, sharing, and community-type functions. They can provide members with an affirmation of the acceptability of abuse conduct and even encourage paedophilia, through the use of euphemisms and seemingly positive terms.[230]

Groups of offenders can also facilitate an exchange of knowledge and tactics for evading law enforcement. Members may, for example, share information about servers located in rogue countries that do not cooperate with international law enforcement, or about the use of encryption methods to conceal incriminating content. Group members might also alert each other with regard to ongoing undercover operations.[231]

Organized criminal groups

Depending upon their structure, offences and aims, groups of child sexual abuse material offenders that exist around online sharing platforms may or may not meet the definition of an organized criminal group for the purposes of the United Nations Convention against Transnational Organized Crime. Article 2 *(a)* of the Organized Crime Convention specifies that an organized criminal group "shall mean a structured group of three or more persons, existing for a period of time and acting in concert with the aim of committing one or more serious crimes or offences established in accordance with the Convention, in order to obtain, directly or indirectly, a financial or other material benefit."[232]

In this respect, the 2013 Cybercrime Study noted that contemporary, online forms of organized crime differ from traditional notions of organized crime that rely upon physical violence and trust-based relations. Instead, ICTs may lend themselves to short-lived networks across vast distances and among offenders who do not have any in-person connection.[233] Some organized criminal groups and individual group members may be involved in both online and offline offences, while others may be involved in online activities only.

In the area of ICT-facilitated child abuse and exploitation, for-profit organized criminal networks are known to be active in the area of child sexual abuse material production and distribution and, in particular, in markets for commercial child sexual exploitation.[234] Organized criminal groups operating in this area may include those based in Asia, South-Eastern Europe, the Commonwealth of Independent States, Mexico and Nigeria.[235] Through the use of ICT, offenders can more easily and less expensively recruit child victims for sexual exploitation, communicate with co-conspirators, and find customers. Groups offering child sex tourism can charge customers for the service of connecting them with their child victims across borders. Increasingly, commercial sexual exploitation of children business operators encourage their customers to pay additional fees for the recording of their exploits in the form of child sexual abuse material.[236]

In a recent United States based survey, 85 per cent of respondents said that they had encountered transnational groups that operate lucrative, profit-motivated child sex abuse material websites.[237] The Commission on Security and Cooperation in Europe noted in a 2006 report that organized crime groups are increasingly using child sex abuse material websites to steal identities and even to extort money from

[229] EUROPOL. European Cybercrime Centre (EC3), 2013. *Commercial Sexual Exploitation of Children Online: A Strategic Assessment*. Available at https://www.europol.europa.eu/sites/default/files/publications/efc_strategic_assessment__public_version.pdf.

[230] Beech, A., et al., 2008. Pp. 221-222.

[231] UNICEF. *Commercial Sexual Exploitation of Children, East Asia and Pacific*. Available at http://www.unicef.org/eapro/activities_3757.html.

[232] Under Article 2 *(c)* of the Organized Crime Convention, a "Structured group" shall mean a group that is not randomly formed for the immediate commission of an offence and that does not need to have formally defined roles for its members, continuity of its membership or a developed structure.

[233] UNODC, 2013. P. 45.

[234] CSCE, 2006. *Combating the Sexual Exploitation of Children*. P.2 Available at. http://digitalcommons.unl.edu/humtraffdata/11.

[235] See e.g. Shelley, L., 2010. *Human Trafficking: A Global Perspective*.

[236] U.S. Department of Justice, 2010. Pp. 25-26.

[237] *Ibid*. P. D-12.

users. Child sexual abuse material consumers are easy targets because they fear police involvement.[238]

Members of commercial groups, by definition, are in the business of distributing child sexual abuse material for financial or other gain. While observers agree that the commercial child sexual abuse material-sector is large, estimates of its exact size vary. The United Nations Special Rapporteur on the sale of children, child prostitution and child pornography estimates that the criminal child sexual abuse material-market generates between US$ 3 billion and 20 billion annually.[239] Other estimates place the market at US$ 250 million per year.[240] Suppliers of child sexual abuse material may specialize in particular types of child sexual abuse material or operate multiple sites to cater to customers' varying demands. Commercial groups may further operate child sexual abuse material websites as a means of obtaining credit card payment information for use in other crimes.

[238] CSCE, 2006. P. 75.

[239] A/HRC/12/23. Paragraph 44.

[240] UNODC, 2010. *Trafficking in Persons to Europe. The Globalization of Crime — A Transnational Organized Crime Threat Assessment*. P. 13. Available at http://www.unodc.org/documents/data-and-analysis/tocta/TOCTA_Report_2010_low_res.pdf.

III. COMBATING THE PROBLEM

This chapter identifies the main international and regional instruments relevant to combating the ICT-facilitated sexual abuse and exploitation of children. The chapter also provides an overview of different practices and policies adopted to combat ICT-facilitated child sexual abuse and exploitation, as well as opportunities to enhance the fight against such crimes.

International instruments

Over the course of the last century, international law has increasingly recognized children as the bearers of rights, and as deserving respect and special protection. Accordingly, several international legal instruments require States Parties to take measures to protect children from abuse and exploitation, as well as to engage in international cooperation in the investigation and prosecution of child abuse and exploitation crimes.[241] The status of ratification, however, varies between instruments, as well as the degree to which the international measures have been incorporated into national law.

United Nations Convention on the Rights of the Child (CRC)

The CRC[242] sets out minimum standards of protection to which children are entitled, including protection from harmful influences, abuse and exploitation. It is one of nine core human rights treaties and almost universally ratified, with 194 States Parties. Specifically, articles 34 to 36 of the CRC require States to protect children from all forms of sexual exploitation and sexual abuse.[243] The Convention requires States Parties to take all appropriate measures at the national, bilateral or multilateral levels to prevent the inducement or coercion of a child to engage in any unlawful sexual activity; the exploitative use of children in prostitution or other unlawful sexual practices; the exploitative use of children in pornographic performances and materials; the abduction of, the sale of or trafficking in children for any purpose in any form; and to protect children against all other forms of exploitation prejudicial to any aspects of their welfare. More broadly, States Parties are obliged to provide appropriate legislative, administrative, social and educational protective measures to ensure the child's safety from all forms of physical or mental violence, injury or abuse, neglect or negligent treatment, maltreatment or exploitation, including sexual abuse (article 18). States Parties are further required to establish social programmes to provide necessary support for the child and for those who have the care of the child, as well as for other forms of prevention and for identification, reporting, referral, investigation, treatment and follow-up of instances of child maltreatment described heretofore, and, where necessary, for judicial involvement (article 18 (2)) and specifically to "take all appropriate measures to promote physical and psychological recovery and social reintegration of a child victim of: any form of neglect, exploitation, or abuse, torture or any other form of cruel, inhuman or degrading treatment or punishment or armed conflicts. Such recovery and reintegration shall take place in an environment which fosters the health, self-respect and dignity of the child" (article 39).

The Optional Protocol to the CRC on the sale of children, child prostitution, and child pornography

While the CRC itself does not specifically and comprehensively address the issue of child (sexual) exploitation, its Optional Protocol on the sale of children, child prostitution, and child pornography (OPSC)[244] focuses exclusively on addressing child sexual abuse and exploitation. The OPSC prohibits the sale of children, child prostitution and child

[241] See UNODC, 2013. Pp. 100-104.

[242] United Nations, *Treaty Series*, vol. 1577.

[243] See generally van Bueren, G., 1995. *The International Law on the Rights of the Child*.

[244] United Nations, *Treaty Series*, vol. 2171 (entered into force on January 18, 2002, 167 States Parties).

pornography as defined in article 2 OPSC[245] and further requires States Parties to adopt and implement legislation criminalizing and adequately punishing at least such acts related to child sexual abuse and exploitation as listed in article 3, being the sale of children, inter alia, for sexual exploitation, offering, obtaining, procuring or providing a child for child prostitution and producing, distributing, disseminating, importing, exporting, offering, selling or possessing child pornography including attempt to and complicity or participation in committing any of the aforementioned acts. Article 3 (4) further requires States Parties to establish criminal, civil or administrative accountability of legal persons with regard to said acts. Concerning the adjudication of child exploitation crimes, article 5, though not excluding any other basis for the exercise of criminal jurisdiction in accordance with international law, stipulates that a State Party shall take all necessary measures to establish its criminal jurisdiction under the principle of territoriality, active and passive personality or the principle of *aut dedere aut iudicare*. Articles 5 and 6 of the Optional Protocol set out general principles for transnational cooperation and extradition in general; article 7 concerns itself with the seizure, confiscation and forfeiture of any goods used to commit or facilitate or any profit derived from the child exploitation crimes set out in article 3; article 8 deals with issues related to victim protection, such as taking due regard of child victims' vulnerability and their entitlement to compensation; and articles 9 and 10 call for the adoption or strengthening of legislative, administrative and political measures and programmes for the prevention of as well as the enhancement of international cooperation with regard to child sexual abuse and exploitation-offences.

United Nations Convention against Transnational Organized Crime

The United Nations Convention against Transnational Organized Crime contains a range of provisions concerning international cooperation against transnational organized crime.[246] It approaches close to universal ratification, with 183 States Parties. It requires Parties to implement a range of measures to facilitate mutual legal assistance, extradition and international cooperation in law enforcement measures. These measures, according to article 3 (1) of the Organized Crime Convention, can be applied to the prevention, investigation and prosecution of any "serious crime," as defined in article 2 *(b)* of the Convention, that is transnational in nature (article 3 (2)), involves an organized criminal group, and is committed with the intent to achieve a material or financial benefit.[247] The term "serious crime" is flexible enough to encompass a range of conduct, including the use of ICTs to abuse or exploit children, if and when the minimum punishment for the specific national crime in question amounts to four years imprisonment or more (article 2 *(b)*). Importantly, in the context of article 3 *(a)*'s definition of the term "organized criminal group", "benefit" has been interpreted to include "sexual gratification, such as the receipt or trade of materials by members of child grooming rings, the trading of children by preferential child sex offender rings or cost-sharing among ring members".[248]

In addition, article 29 (1) *(h)* of the Organized Crime Convention requires States parties, to the extent necessary, to "initiate, develop, or improve specific training programmes for its law enforcement personnel" on the "methods used in combatting transnational organized crime committed through the use of computers, telecommunications networks or other forms of modern technology".

[245] "For the purposes of the present Protocol: *(a)* Sale of children means any act or transaction whereby a child is transferred by any person or group of persons to another for remuneration or any other consideration; *(b)* Child prostitution means the use of a child in sexual activities for remuneration or any other form of consideration; *(c)* Child pornography means any representation, by whatever means, of a child engaged in real or simulated explicit sexual activities or any representation of the sexual parts of a child for primarily sexual purposes": Sweden clarified its position regarding the interpretation of child pornography in this context as only applying to the visual representation of sexual acts with a child or minor persons, and not applying to adults acting, posing, or dressing, as a child [*Official Records of the General Assembly, Fifty-fourth Session* (A-54-PV.97)].

[246] United Nations, *Treaty Series*, vol. 1577 (entered into force on September 23, 2003).

[247] See also Petty, K. A., 2011. "Protecting Children from Cyber Crime: The Twentieth Session of the United Nations Commission on Crime Prevention and Criminal Justice", *American Society of International Law: Insights* 15, No. 24. Available at http://www.asil.org/insights/volume/15/issue/24/protecting-children-cyber-crime-twentieth-session-un-commission-crime.

[248] *Ibid.*

The Protocol to Prevent, Suppress, and Punish Trafficking in Persons, Especially Women and Children

The Protocol to Prevent, Suppress, and Punish Trafficking in Persons, Especially Women and Children, supplementing the United Nations Convention against Transnational Organized Crime requires its 165 States Parties to criminalize the trafficking of persons, including children. It also contains provisions relating to the prevention and combating of trafficking, the protection and assistance of victims of trafficking and to international cooperation between States Parties in order to meet those objectives. A key value of the Protocol lies in the fact that it renders irrelevant the consent of any child victim of the practice of trafficking in persons within the scope and meaning of article 3 *(a)*, stipulating that "the transportation, transfer, harbouring or receipt of a child for the purpose of exploitation shall be considered 'trafficking in persons' even if this does not involve any of the means set forth in subparagraph *(a)*". In other words, a child, and even the child's custodians, cannot ever validly consent to the child being trafficked or exploited because of the special legal status afforded to children.[249] In terms of assisting and protecting child victims of trafficking, the Trafficking in Persons Protocol specifies in article 6(4), that "each State Party shall take into account, in applying the provisions of this article, the age, gender and special needs of victims of trafficking in persons, in particular the special needs of children, including appropriate housing, education and care".

Guidelines on Justice in Matters involving Child Victims and Witnesses of Crime

The Guidelines on Justice in Matters involving Child Victims and Witnesses of Crime,[250] adopted in 2005 by the United Nations Economic and Social Council, set forth "good practices based on the consensus of contemporary knowledge and relevant international and regional norms, standards and principles." They are intended to provide governments, law- and policymakers, civil society and practitioners, especially the judiciary, with a practical framework for adopting adequate legislation, policies and practices, in order to ensure full respect for the rights of child victims and witnesses of crime. The Guidelines also seek to contribute to the effective implementation of the CRC and to assist, support and improve the assistance, treatment and care for child victims so as to meet these children's special needs and best interests. The principles and guidelines are relevant with regard to the sexual exploitation and abuse of children insofar as they also pertain, in general, to victims of abuse and exploitation crimes within or without the context of ICTs. Moreover, some specific guidelines, such as ones related to the right to privacy, the right to protection from hardship and the right to safety, are essential in affording child victims and witnesses of sexual abuse and exploitation a due amount of protection against re- and secondary victimization.

Regional instruments

Council of Europe Convention on Cybercrime

The Council of Europe Convention on Cybercrime[251] aims to provide a common criminal policy aimed at the protection of society against cybercrime. With respect to the substantive criminal law provisions of the Convention, some ICT-facilitated child exploitation offences fall within the scope of article 9, which deals with offences related to child pornography.[252] The Convention currently has 42 States Parties, including 6 non-members of the Council of Europe.[253]

Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse

The Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse[254] ("Child Sexual Abuse Convention") aims to prevent and combat sexual exploitation and sexual abuse of children, protect the rights of child victims of sexual exploitation and sexual abuse, and to promote national and international cooperation against sexual exploitation and sexual abuse of children (article 1).

Alongside adopting specialized protective and preventive measures, measures to provide assistance to victims and

[249] See, for example, UNODC, 2006. Toolkit to Combat Trafficking in Persons: Global Programme against Trafficking in Human Beings. Pp. xv-xviii. Available at http://www.unodc.org/documents/human-trafficking/HT-toolkit-en.pdf.

[250] ECOSOC Resolution 2005/20.

[251] CETS No.185.

[252] UNODC, 2013. Pp. 100-104.

[253] http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG.

[254] CETS No. 201 (entered into force on July 1, 2010 and currently ratified by 30 Parties, including some non-Member States of the Council of Europe and the EU).

appropriate and effective counter-policies, States Parties are required to criminalize conduct related to the sexual abuse and exploitation of children as specified in articles 18 to 23 by either natural or legal persons as well as the attempt to commit and complicity or participation in such conduct (article 24).[255] Specifically with regard to ICT-facilitated child sexual abuse and exploitation, article 20 (1) *(f)* obliges States Parties to criminalize knowingly obtaining access to, through information and communication technologies, child pornography and the intentional proposal, through information and communication technologies, of an adult to meet a child who has not reached the legal age for sexual activities under national law for the purpose of intentionally engaging in sexual activities with such a child (article 18 (1) *(a)*), or intentionally and unrightfully producing child pornography (article 20 (1) *(a)*), against him or her, where this proposal has been followed by material acts leading to such a meeting. Although the provisions on the interdiction of child pornography also pertain to simulated, (such as digitally or virtually created) material (article 20 (2)), the Convention allows States Parties to refrain from criminalizing material consisting exclusively of simulated representations or realistic images of a non-existent child (article 20 (3)).

African Charter on the Rights and Welfare of the Child

Article 27 of the African Charter on the Rights and Welfare of the Child requires States Parties to undertake to protect children from all forms of sexual exploitation and sexual abuse, and, in particular, to take measures to prevent the inducement, coercion or encouragement of a child to engage in any sexual activity, the use of children in prostitution or other sexual practices and the use of children in pornographic activities, performances and materials. Article 15 calls for the protection of children from all forms of economic exploitation and from performing "any work that is likely to be hazardous or to interfere with the child's physical, mental, spiritual, moral, or social development" and commits States Parties to "take all appropriate legislative and administrative measures to ensure the full implementation of this Article which covers both the formal and informal sectors of employment and having regard to the relevant provisions of the International Labour Organization's instruments relating to children". Furthermore, article 16 obliges States Parties to "take specific legislative, administrative, social and educational measures to protect the child from all forms of torture, inhuman or degrading treatment and especially physical or mental injury or abuse, neglect or maltreatment including sexual abuse, while in the care of the child".

National laws and policies

As noted in the Cybercrime Study, although 80 per cent of countries in Europe report sufficient criminalization of cybercrime acts, in other regions of the world, up to 60 per cent of countries report that criminalization of cybercrime acts is insufficient.[256]

States vary considerably in their approach to addressing the various forms of child abuse and exploitation. While many States criminalize acts such as production of child sexual abuse material, they may differ on the concrete elements of the crime and the definitions of "child". While children are the victims in all of these crimes, child sexual abuse material and child sexual exploitation crimes deal first and foremost with contact sexual abuse of children in which the ICT component can be seen as re-victimization and/or evidence of an ongoing crime. While child sexual abuse material laws may contain ICT-specific components, laws against child sexual exploitation and trafficking in children typically do not, with the result that these crimes may be dealt with by the application of more general criminal offences.[257]

Acts such as cybergrooming, -solicitation, -stalking, -harassment, -bullying and exposure to harmful content have been dealt with both by enacting new offences, as well as through the application of existing offences. Indeed, information contained in the Cybercrime Study indicates that computer-related acts causing personal harm, as well as computer-related solicitation or grooming, are more often criminalized using general offences than cyberspecific ones.[258] Some issues—in particular such as cyberbullying—have also been addressed through non-legislative approaches, such as awareness-raising initiatives to educate on online risks or parental controls to limit children's usage of certain devices, track devices' location or activity or control access to certain material.[259] According to an OECD report on the Protection

[255] See also E/CN.15/2011/2.

[256] UNODC, 2013. Chapter 4.

[257] See also OECD, 2012. 32-34, 39-44; UNODC, 2013. Pp. 100-106.

[258] See UNODC, 2013. Pp. 100-106.

[259] *Ibid.*

of Children Online, government policies in this area are in their infancy.[260]

Several countries have also devised national strategies or developed policy frameworks which address child protection in the light of new challenges raised by the Internet. These often seek to combine and coordinate measures involving various stakeholders.[261] At the national level, efforts to prevent and combat such crimes also require effective inter-agency coordination.[262]

In many countries, there may be little to no legal basis for police to take action against child abusers and exploiters if the victim has already reached the legal age of consent, even though the child is still under 18 years of age. Most jurisdictions still set the age of consent for sexual activity below 18 years of age, with the average ranging from 13 to 16 years.[263] Importantly, some countries' laws make the permissibility of sexual intercourse and other related practices dependent on the age difference between partners or on whether the partners are married, whereas others rely on notions such as gauging when a child has reached puberty. Still others do not specify any age of consent at all. To complicate the matter further, countries have different definitions for sexual activity, ranging from kissing to sexual intercourse.[264] The definition of "child" in domestic legislation as well as the criminal provisions on sex crimes are critical issues in all matters relating to child protection and combatting child sexual abuse and exploitation.

Child sexual abuse material

Surprisingly, child sexual abuse material has come to the attention of criminal law only comparatively recently, with laws in countries such as England, Canada and the United States only entering into force in the late 1970s. Laws against child sexual abuse material in most countries are based on the policy position that children should be protected from commercial sexual activities because they are too young to give informed and thus valid consent.[265]

States define offences related to child sexual abuse material in varying ways.[266] For example, in some countries, (adult) pornography is considered to be an offence against public morals and decency or a violation of public order, and child pornography is punished in that context. Other countries link child pornography to obscenity laws that cover a wide range of different images, only some of which may be illegal.[267] A common approach in Western and Northern countries is to criminalize only child sexual abuse material (and not pornography in general) on the basis of the age, or apparent age, of victims.

As indicated in the Cybercrime Study, interests protected by the criminalization of child abuse images include the protection of minors from abuse, and the disruption of commercial markets in child abuse images, that may encourage offenders to seek to produce and supply further images. Although international frameworks demonstrate many similarities with respect to the criminalization of child pornography, differences also relate to the object, age of children and acts covered.[268] The Cybercrime Study also found that, at the national level, over 80 per cent of countries responding to the Study questionnaire indicated that child pornography is a criminal offence. The majority of countries reported that computer-related acts are criminalized by way of a general offence.[269] As an example, in Mauritius, offences against children can be prosecuted under laws related to, inter alia, rape, sexual intercourse with minors under the age of 16, attempts upon chastity, sodomy, alleged sexual assault, causing a child to be sexually abused, accessing a brothel, child abduction, attempts upon chastity of minors under the age of 12, as well as under the Computer Misuse and Cybercrime Act of 2003.[270]

---

[260] See also OECD, 2012. Pp. 32-34.

[261] In Mauritius, for instance, in order to promote the cooperation and coordination among ministries and institutions in the field of child protection, a protocol of collaboration for the promotion of children's rights and their protection against abuse, including commercial sexual exploitation, has been signed by relevant stakeholders. Comments from experts, Government of Mauritius, April 2014.; see also OECD, 2012. Pp. 39-44.

[262] See also OECD, 2012. P. 47.

[263] ECPAT, 2008. *Strengthening Laws Addressing Child Sexual Exploitation: A Practical Guide*. Pp 47-50. Available at http://www.ecpat.net/sites/default/files/Legal_Instrument_En_Final.pdf.

[264] Ibid.

[265] Subgroup Against the Sexual Exploitation of Children, 2005.

[266] A/HRC/12/23.

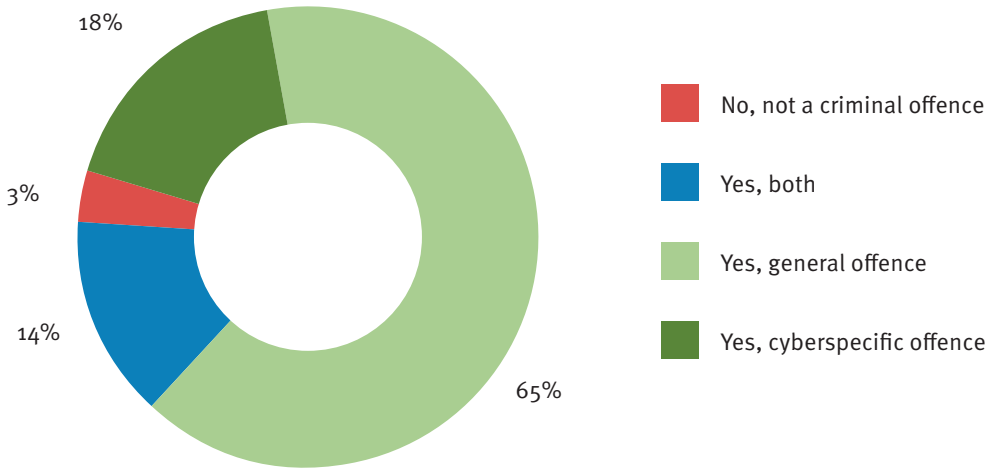
[267] UNODC, 2013. 100-104; Subgroup Against the Sexual Exploitation of Children, 2005. Pp. 29.

[268] UNODC, 2014. Pp. 100-104.

[269] *Ibid.*

[270] Comments from experts, Government of Mauritius, April 2014.

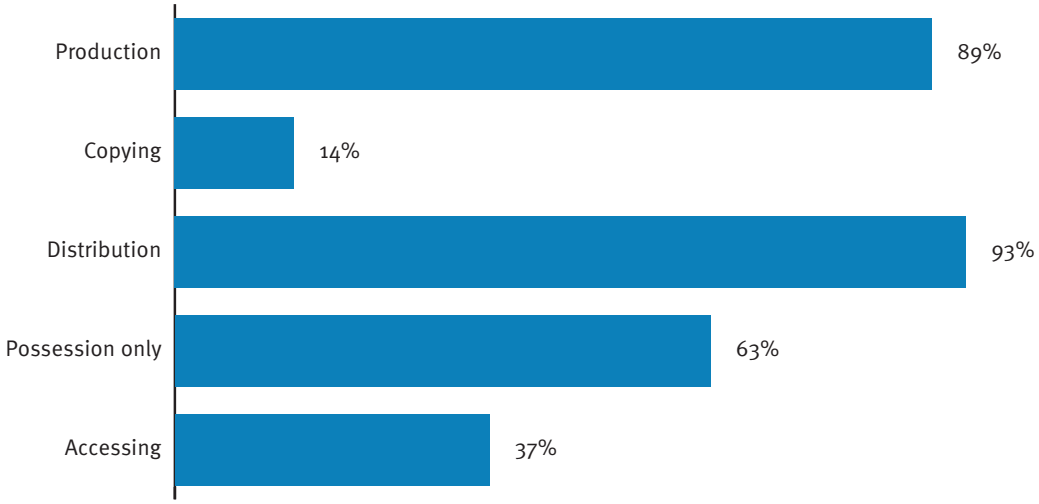
Figure IV. Criminalization of computer-related production, distribution or possession of child pornography



Source: Study cybercrime questionnaire, Q36 (n=57).

While the majority of international and regional instruments require criminalization of a wide range of actions associated with child pornography, including "production", "offering", "making available", "distribution", "transmission", "possession" and in some instances also knowingly "obtaining access" to child pornography, national laws show some diversity with respect to which of these acts are included. As described in the Cybercrime Study, the production and distribution of child pornography are criminalized by around 90 per cent of national legislative provisions reviewed; in addition, over 60 per cent of

Figure V. Acts constituting child pornography offences



Source: UNODC legislation review (n=70).

countries criminalized "possession", with almost 40 per cent including provisions on "accessing" child pornography.[271]

One issue surrounding the criminalization of child sexual abuse material relates to its inadvertent possession. Some States have resolved this by broadly interpreting possession to include any exercise of dominion or control over images, including such contained in digital Internet "cache" files. Policymakers in the United States and South Africa have also noted, for instance, that punishment of non-contact offenders in these countries is based on the concern that the distribution and viewing of child sexual abuse material may incite more contact abuse.[272]

One of the most prevalent distinctions made by national legal systems is that between contact and non-contact offences. National laws against child sexual abuse material are primarily grounded in the suffering caused by the original sexual abuse, and so tend to mainly focus on contact offences. A number of countries, however, give weight to both contact and non-contact offences, taking into consideration not only the original abuse, but also its implications in the form of the suffering of victims from the potentially infinite dissemination of abuse images. Finland and Slovakia,[273] for example, have some of the most restrictive laws in this regard.[274] Some States have also successfully prosecuted citizens for contact sexual abuse offences conducted through live web streaming of child sexual abuse material, holding that directing live commercial sexual exploitation via the Internet is equal to rape of a child.[275]

Some States may have no laws that specifically criminalize child sexual abuse material.[276] Countries without specific laws may nonetheless criminalize the production, distribution or possession of this type of material under broader laws related to obscenity, decency and vice.[277] Countries also vary in their treatment of "virtual" and "simulated" child sexual abuse material. "Virtual" child sexual abuse material generally refers to visual material that appears to depict children engaged in sexual acts but that is actually the product of digital creation, animation, morphing or composite making. "Simulated" child sexual abuse material refers to materials featuring adults who are disguised to look like children. Whereas some States penalize possession of virtual child sexual abuse material to a lesser extent than that of real child sexual abuse material, others do not make such a distinction. Results from the Cybercrime Study showed that national laws on child pornography use a range of terminologies, but only in around one-third of countries do they include simulated material.[278] Countries such as Sweden and the United States, for example, do not criminalize simulated child sexual abuse material because children were not involved in its production, while other countries do criminalize this material because the simulated material is difficult to distinguish from real child sexual abuse material and may stimulate the market for the latter.

[271] UNODC, 2013. Pp. 100-104; ECPAT, 2008. Pp. 81-88.

[272] *Ibid*.

[273] A/HRC/12/23. Paragraphs 56-57.

[274] Arguably these countries may treat as criminal acts of possession, the watching of online child sexual abuse material because the material is temporarily stored in the computers' cache of viewers; see ECPAT, 2008. Pp. 8388; UNODC, 2013. P. 103.

[275] EUROPOL, 2013.

[276] A/HRC/12/23. Paragraph 53.

[277] UNODC, 2013. Pp. 100-101.

[278] *Ibid*. Pp. 102.

Figure VI. Criminalization of the computer-related production, distribution or possession of simulated child pornography

Source: UNODC legislation review (n=70).

The United States grappled with the issue of virtual and simulated child sexual abuse material in 2002 when the Supreme Court in *John D. Ashcroft Attorney General, et al v. The Free Speech Coalition, et al.*[279] repealed the prohibition on virtual child sexual abuse material contained in the Child Pornography Prevention Act of 1996. On that occasion, the Supreme Court struck down as unconstitutional a definition of child sexual abuse material that included images that merely "appear to be" of a minor engaged in sexually explicit conduct. Almost immediately thereafter and in response to this decision, the United States Congress adopted the "Prosecutorial Remedies and Other Tools to End the Exploitation of Children Today Act of 2003" (PROTECT Act). In addition to prohibiting "real" child sexual exploitation images, the PROTECT Act also includes prohibitions against: *(a)* any digital or computer-generated image that is "indistinguishable" from that of a minor engaging in sexually explicit conduct; and *(b)* a visual depiction that has been created or modified to appear as an identifiable minor engaging in sexually explicit conduct.

Commercial sexual exploitation of children

UNICEF has reported gaps concerning child prostitution in the criminal laws of many States Parties to the OPSC. These gaps include laws that only criminalize the prostitution of children below the age of consent to sexual activity in the national legal system or that define prostitution in gender-specific terms, or exclude certain sexual acts. For example, national legislation on trafficking often focuses on sexual exploitation of women and girls, which neglects trafficking of boys for sexual exploitation. The laws of some countries focus on the immorality of sexual activities rather than the exploitation and abuse that have occurred. As a result, trafficking survivors may be held legally accountable for acts committed as a result of sexual exploitation.[280]

With regard to the existence of specific anti-trafficking legislation, according to the 2012 UNODC Global Report on Trafficking in Persons, more than 90 per cent of the 162 countries and territories covered by the report had such legislation covering fully or partially, all or most forms of trafficking in persons. This means that at least 134 countries and territories in the world have criminalized trafficking and established a strong legislative basis for cooperation, exchange of good practices and a common understanding of what trafficking in persons is and that victims of this crime are to be protected. An additional 19 countries have legislation covering trafficking in persons partially, either by focusing on women or children only, or by covering one type of exploitation only, such as sexual exploitation.[281] Some States make trafficking in children an aggravating factor, or specify an enhanced penalty for such acts.[282] Although legislation rates have increased substantially

[279] U.S. Supreme Court, Case No. 00-795.

[280] UNICEF, 2009. *Handbook on the Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography*. Pp. 23-24.

[281] UNODC, 2012. *Global Report on Trafficking in Persons*. Pp. 82-83.

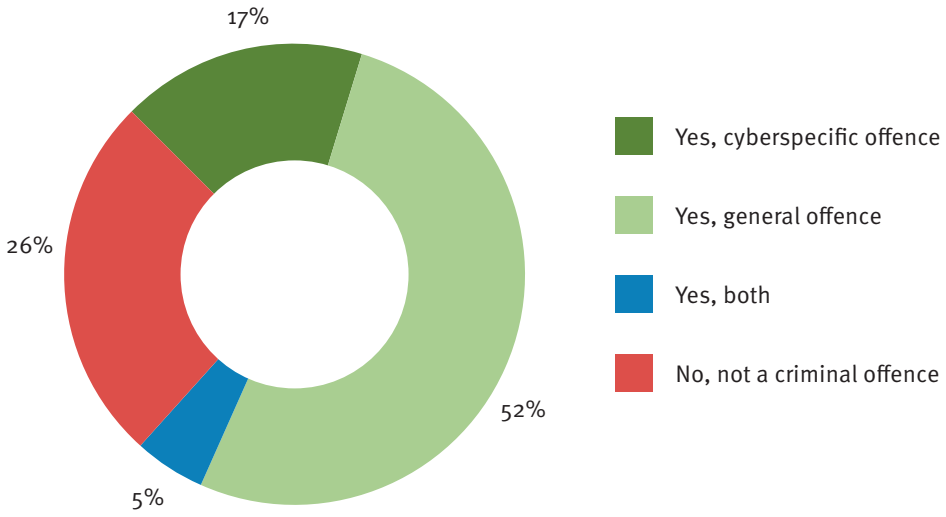
[282] UNODC. *Model Law against Trafficking in Persons* (United Nations publication, Sales No. E.09.V.11).

in the last ten years, conviction rates remain very low, indicating that effective implementation of anti-trafficking laws is difficult to achieve, leaving children vulnerable to ICT-facilitated trafficking for sexual exploitation and abuse.[283]

Cyberenticement, solicitation or online grooming

Reports of cases of cyberenticement or online grooming have increased in recent years. The Cybercrime Study found that almost 70 percent of countries criminalize this offence although most of the laws pertain to general and not to cyber-specific offences.[284] The Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, which has been ratified by 31 Council of Europe-countries, in article 23 specifically requires States Parties to enact legislation that criminalizes this conduct. As the nature and prevalence of grooming offences becomes better known, additional States may enact criminal laws against it.

Figure VII. Criminalization of computer-related solicitation or "grooming" of children



Source: Study cybercrime questionnaire, Q37 (n=54).

New Zealand's Harmful Digital Communications Bill

The legislation, now before the New Zealand parliament, would make it an offence to send or post harmful messages—punishable by a $2,000 fine or three months' jail time—and create a specialized enforcement agency to deal with cyberbullying complaints. Inciting someone to commit suicide over the Internet would be illegal, carrying a maximum three-year jail sentence.

The United States Children's Internet Protection Act (CIPA)

CIPA was enacted in 2000 to address concerns about children's access to obscene or harmful content over the Internet. CIPA imposes certain requirements on schools or libraries that receive discounts for Internet access or internal connections.

Schools and libraries subject to CIPA may not receive such benefits unless they have in place protection measures that block or filter Internet access to pictures that are: *(a)* obscene; *(b)* child pornography; or *(c)* harmful to minors (for computers that are accessed by minors). Before adopting this Internet safety policy, schools and libraries must provide reasonable notice and hold at least one public hearing or meeting to address the proposal.

[283] See also UNODC, 2012. Pp 82-88; UNICEF, 2009. P. 24.

[284] UNODC, 2013. P. 104.

Cyberbullying, stalking and harassment

Few countries have specific legal regimes that address online harassment offences, such as cyberstalking, harassment or bullying. With respect to cyberstalking, many countries do not consider voyeurism or invasion of privacy to be criminal offences, particularly when they occur exclusively online. Nearly all States do, however, criminalize stalking conduct that escalates into kidnapping, threats of violence, or any kind of contact offence. Some states have adopted laws that a communication must evidence a serious expression of an intention to inflict bodily harm as perceived by a reasonable person. Nonetheless, the growth of social networks, as well as recent child suicide cases possibly linked with cyberbullying, have raised new concerns about the expansion of the phenomenon. Policy dialogue concerning the appropriateness of any criminal justice response where the perpetrator is also a minor, as well as the nature of effective education and prevention approaches, represents an urgent need in this area.

Limiting children's exposure to harmful content

Many of the initiatives to combat exposure of children to harmful content focus on non-statutory forms of regulation. In many territories, models are being developed that allow for greater co- and self-regulation with and by the private sector. These initiatives suggest that the implementation of measures, such as those to protect children from potential harm, can be implemented efficiently and speedily, while being accepted by the stakeholders in this process. One model is co-regulation. This is a generic term for cooperative forms of regulation that are designed to achieve public objectives and that contain elements of self-regulation as well as of traditional legal regulation. The other model, self-regulation, is the process whereby industry actively participates in and is responsible for its own regulation, while remaining subject to the general rule of law. The basic elements of self-regulation include a code of practice or guidelines adopted by the industry processes by which application of the code or principles may be assessed a complaints resolution process, including sanctions.[285]

Investigation of ICT-facilitated child abuse and exploitation

At the same time as ICT offers a sense of anonymity to perpetrators, and can present some challenges to offender identification, it also offers many opportunities for law enforcement investigations, including through the generation of clear evidence trails. This section considers the use of image analysis and image databases, digital forensics, automated search, data mining and analytics, and undercover operations in the investigation of ICT-facilitated child abuse and exploitation.

Image analysis and image databases

A critical function of law enforcement in regard to ICT-facilitated abuse and exploitation of children is the ongoing effort to rescue unidentified victims seen in online material. Technologies such as Microsoft's "PhotoDNA" are vital in helping law enforcement quickly identify "known" images. Prior to the development of such software, the ability of investigators to automatically compare suspects' image collections to databases of known representations of child sexual abuse was limited. This was due primarily to the fact that previous software was based on hash-value comparison technology, which only matched images that were exactly identical, so that even minimal alterations, such as stretching the dimensions, flipping the orientation of the image, changing the coloration, or even changing the file names, would render the image undetectable in automated search processes. In comparison, PhotoDNA, which is available to law enforcement free of charge, creates a unique signature for a digital image, something like a fingerprint, which can be compared with the signatures of other images to find copies of that image.[286]

Other software developers have also deployed technical innovations to combat the proliferation of child sexual abuse material by working to enable ISPs to algorithmically find and remove child sexual abuse material from their servers. Such products are also employed by governments to conduct investigations, and private sector enterprises to

[285] Andrea Millwood Hargrave, 2009. *Protecting children against harmful content. Report prepared for the Council of Europe's Group of Specialists on Human Rights in the Information Society*. Available at https://www.bka.gv.at/DocView.axd?CobId=40268.

[286] Latonero M., 2011. *Human Trafficking Online: The Role of Social Networking Sites and Online Classifieds* (2011). Pp. 31-32. Available at http://dx.doi.org/10.2139/ssrn.2045851.

eliminate child sexual abuse material from search results and communications.[287]

INTERPOL and the United States-based National Center for Missing and Exploited Children (NCMEC) have further developed databases of abuse images that include information on identified and unidentified victims. These databases can help to reduce redundancy in investigative efforts, while serving the interests of victim-protection. They enable prioritization of work on unidentified victims and ensure that only investigators trained to handle child sexual abuse material may access them. In addition, image databases enable law enforcement agencies to triage their forensic investigations by comparing suspects' digital materials to images in databases through using hash analysis or PhotoDNA.[288]

INTERPOL's International Child Sexual Exploitation Image Database was recently launched with a view to identifying and rescuing previously unidentified victims. The Database makes use of sophisticated image comparison software to make connections between victims and places.[289] Equipped with information about the nexus between images and locations, investigators can more easily work to identify offenders.[290] By the end of 2013, more than 3,000 victims from more than 40 countries, and more than 1,500 offenders, had been identified and recorded in the database.[291] An example of the impact of this technology in practice comes from a recent undercover operation that used the INTERPOL Database to target 55 suspects using social network sites for trading child pornography. The offenders came from 19 different countries, requiring close cooperation between law enforcement agents in those countries. Twelve children were rescued as a result of the operation.[292]

The National Center for Missing and Exploited Children (NCMEC) also houses a database of victims who have been identified through previous cases. Such data is essential to support cases that require proof that the children depicted in child sexual abuse material are indeed real children and not the product of digital animation. To date, NCMEC has processed more than 15 million photos and videos. According to a 2009 report of the United Nations Special Rapporteur on the sale of children, child prostitution and child pornography, as of 2009, NCMEC had identified 592,044 out of a total of 681,275 sites as child sexual abuse material sites. Shared access to the NCMEC database has enabled law enforcement agents around the world to rescue more than 1,600 children.[293]

The United Kingdom Child Exploitation Online Protection Centre is also in the process of rolling out a national image bank. This database is focused on cases that originate in the United Kingdom or that involve victims from that country. To date, it has helped to rescue 18 children.[294]

Digital forensics

User interaction with computer devices produces a wealth of computer-generated digital traces. Digital forensics is the branch of forensic science concerned with the recovery and investigation of such material found in digital and computer systems. Computer data and electronic communications potentially relevant to a criminal act may include large volumes of photographs, videos, emails, chat logs and system data. Locating relevant information within this data can be extremely time-consuming. The variety of possible file formats, operating systems, application software, and hardware particulars also serves to complicate the process of identifying relevant information. To recover such traces, digital forensics experts make use of a range of investigative and forensic techniques. Examination of mobile devices requires a different set of tools to those employed when examining a desktop computer or network server. Varying types of hardware, software and operating systems each present their own challenges associated with retrieving information.[295]

Automated search

Automated searches enable forensic investigators to easily and quickly find sites and content displaying child sexual abuse relating to Internet content which are tagged with

[287] See, for example, http://www.netclean.com/en/about-us/our-products/; see also Ungerleider, N., 2013. How Mobile Phones And The Internet Fight (And Help) Human Trafficking, 8 January 2013. Available at http://www.fastcoexist.com/1681155/how-mobile-phones-and-the-Internet-fight-and-help-human trafficking.

[288] A/HRC/12/23. Paragraphs 78-80.

[289] http://www.interpol.int/Crime-areas/Crimes-against-children/Crimes-against-children.

[290] A/HRC/12/23. Paragraphs 78-80.

[291] http://www.interpol.int/Crime-areas/Crimes-against-children/Victim-identification.

[292] CNN Wire Staff, "INTERPOL Targets 55 Suspects Using Social Networking Sites for Child Sex Abuse Images", 22 March 2012. Retrieved from http://article.wn.com/view/2012/05/23/INTERPOL_targets_55_suspects_using_social_network_sites_for_/.

[293] A/HRC/12/23. Paragraph 80.

[294] *Ibid*. Paragraph 81.

[295] UNODC, 2013. Pp. 157-161.

commonly used keywords, including potential misspellings. Searches can also be made by file type, size, creation date and other traits. Commercial programmes and customized macros can also be used to automatically initiate and carry out common or regular searches. These ICT-facilitated searches can yield a valuable basis for further "manual" investigation, which in turn might serve as a starting-point for further ICT searches.

Data mining and analytics

The massive amount of data available on the Internet can be used to assist in the prevention, detection, and prosecution of child exploitation crimes. In this context, data mining[296] and analytics have undergone tremendous advancements in recent years.[297] Over the last decade in particular, both businesses and governments have prioritized the development and deployment of technology tools that enable conceptual link analysis. This can be used in the fight against child sexual abuse and exploitation through the use of software that can quickly search and analyse thousands of distinct databases, financial records, DNA samples, sound samples, video clips, maps, floor plans and human intelligence reports and weave together relevant data into an accurate, coherent and useful trajectory. In particular, social networking companies may be able to identify the kinds of profile that most commonly trigger contact by offenders, and to undertake preventive or educational measures, or to share information with law enforcement authorities in response to requests made through due legal process.

Data mining and analytics companies often work to continuously improve their software's ability to assemble relevant information in a law enforcement context. One large data analytics company, for example, worked with a child abduction resource centre to link an attempted abduction to previous hotline reports displaying similar traits. In a matter of minutes, the software had linked the relevant data from various databases and plotted the information on a map, which the investigative team could use to locate the suspect more quickly.[298]

In another example, researchers conducted an experiment by searching on the keyword "escort" during the Superbowl on Twitter. The voluminous and data-rich search results showed that investigators could effectively use data analysis and visualization tools to effectively narrow down the pool of advertisements that more likely involved trafficking situations. Such results have galvanized research on new means of using social media to prevent all kinds of crime, including child trafficking.[299]

Undercover operations

Online crimes can be especially suitable for undercover work as—compared to the investigation of offline drug trafficking or organized crime syndicates—investigators are not required to alter their appearance, to invest months or even years establishing a cover identity, or even to devote themselves to the undercover investigation permanently.

The most common methods of undercover investigations in ICT-facilitated child abuse and exploitation consist of law enforcement agents posing as children, virtually entering chat rooms, setting up false websites that purport to display child sexual abuse material, or joining child sexual abuse material communities purporting to be a child sexual abuse material consumer. Several factors impact the success of such operations. Just as in the real world, the agents conducting such cyber-investigations must not only be fluent in the potential child victims' lingo , such as current slang terms and common Internet chat terms such as TTYL (talk to you later) or LOL (laughing out loud), but must also have profound expertise in how sophisticated targets could trace and verify their identity.

Mechanisms for international cooperation

The 2013 Cybercrime Study noted that use of traditional cooperation predominates for obtaining extra-territorial evidence in cybercrime cases.[300] Formal international cooperation mechanisms such as mutual legal assistance—the process whereby States formally request judicial assistance from another State in criminal investigations—may often similarly be used in transnational investigations of ICT-

[296] Data mining is the searching of large data sets to identify patterns that can inform decision-making.

[297] Clifton, C. Definition of Data Mining. In Encyclopedia Britannica, 2010.

[298] Vance, A., Stone, B., 2011. Palantir, the War on Terror's Secret Weapon. Business Week, 22 November 2011. Available at http://www.businessweek.com/magazine/palantir-the-vanguard-of-cyberterror-security-11222011.html#p3.

[299] Latonero, M., 2011. Pp. 23-26.

[300] UNODC, 2013. P. 197.

facilitated abuse and exploitation. At the same time, however, the importance of victim identification and protection, as well as the need for timely information sharing has resulted in the development of effective cooperation mechanisms at the operational law enforcement, as well as strategic levels.

With regard to volatile computer data and at-risk children, both of which require immediate action by law enforcement, police often need to attain information or assistance faster than they could via formal channels, such as mutual legal assistance. Informal direct communication between police officers can provide a valuable supplement to formal procedures. While waiting for official responses to information requests, police can advise each other on how to follow up time-sensitive leads. They may also be able to inform each other about cultural norms and local practices, which may facilitate cross-border investigations.[301]

An example of a successful international law enforcement operation

Particularly with regard to child sexual abuse material, international law enforcement operations have been instrumental in increasing arrests and convictions and bringing awareness of the crime. One of the first such operations, Operation Avalanche as it was called in the United States, was initiated in 1999 and was set up to examine the 35,000 names registered to a pornography web-portal database. The United States Federal Bureau of Investigation shared the details of subscribers from overseas with law enforcement agencies in the relevant countries and operations were initiated in Canada, Germany, Ireland, Switzerland and the United Kingdom. In total, 59 countries were involved in this investigation. This type of cooperation has been replicated successfully many times since and does not generally involve sustained coordination or action, or requests for legal assistance through formal or informal channels. Sustained joint operations as well as mutual legal assistance procedures are types of international cooperation that are frequently more complicated and time consuming to implement.

The Cybercrime Study reported that, while many countries engage in informal cooperation in cybercrime cases, the range of investigative actions that can be provided through such channels varies considerably, as well as the existence of clear policies on its use. One major problem in the context of informal cooperation is the fact that many countries prohibit the use of evidence obtained through such informal channels in the context of judicial proceedings. Nevertheless, "24/7" networks in particular hold a considerable potential for streamlining informal cooperation and facilitating formal cooperation; however, they still tend to be used infrequently in the investigation and prosecution of transnational cybercrime. The Cybercrime Study also concluded that, globally, divergences in the scope of cooperation provisions contained in multilateral and bilateral instruments, a lack of response time obligation, multiple informal law enforcement networks and variance in cooperation safeguards represent significant challenges to effective international cooperation regarding electronic evidence in criminal matters.[302]

At the strategic level, the formation of multi-agency partnerships has emerged as a common practice for combating technology-facilitated crimes against children. Groups such as the Virtual Global Task Force (VGT), the Financial Coalition against Child Pornography (FCACP), and the International Association of Internet Hotlines (INHOPE) bring together different agencies from multiple countries to work on specific child exploitation issues. Such initiatives aim to harness the ideas and resources of multiple entities, resulting in more robust policy and programme initiatives.[303] Forums for information-sharing and joint problem-solving are also examples of commonly adopted practices for combating online child abuse and exploitation.

Working groups sponsored by private entities, individual States, and regional and international coalitions constitute important opportunities for detailed technical information exchange. The INTERPOL Specialist Group on Crimes Against Children, for example, brings together global experts to share best practices. Individuals involved benefit from opportunities for developing informal relationships that may facilitate fast and easy cross-border cooperation in the future.[304]

[301] UNODC, 2013. Pp. 208-215.

[302] UNODC, 2013. Pp. 197-215,

[303] See, for example, http://www.inhope.org/gns/Internet-concerns/overview-of-the-problem/illegal-content.aspx; http://www.virtualglobaltaskforce.com/what-we-do/.

[304] http://www.interpol.int/Crime-areas/Crimes-against-children/Crimes-against-children.

Regional coalitions have also emerged. For example, in April 2009, national coalitions and NGOs from seven countries (Costa Rica, El Salvador, Guatemala, Honduras, Mexico, Nicaragua and Panama) adopted a declaration following a seminar on the development of comprehensive strategies to combat child pornography. These seven countries adopted a declaration on the development strategies to combat child pornography.[305]

Prosecution of ICT-facilitated child abuse and exploitation

In many States, new procedures reduce the likelihood of secondary victimization of child victims by abolishing the need for victims or witnesses to repeatedly testify to multiple parties. Procedures for eliciting reliable testimony while minimizing further trauma have also emerged, including the use of pictures and dolls for young children to relate their experiences, as well as the establishment of comforting, age-appropriate spaces for interviews. A number of States have specific laws and procedures designed to protect a child victim or witness, including bars on reporting of identity, non-public hearings or sections of hearings, giving of testimony from remote location or via video-recording, physical security protection, as well as the availability of psychosocial support. Victims may also often have the right to be kept informed of the progress of proceedings on a timely basis and to make victim impact statements.

Similarly, investigators and prosecutors increasingly use ICTs to corroborate victims' accounts, through other forms of digital evidence such as hotel receipts, "trick books," or note books and mobile telephone records. Moreover, in trials concerning the commercial exploitation of children, just as in those of other exploitation and abuse crimes, prosecutors may rely on expert witnesses to inform judges and juries on the techniques offenders use to establish and maintain control over their victims and the impact of these crimes on victims.

[305] A/HRC/12/23. Paragraph 118.

Private sector responses

Self-regulation in the private sector

In addition to the development of tools to detect and investigate ICT-facilitated child abuse and exploitation, the private sector can also engage to varying degrees in "self-regulation" in order to help combat ICT-facilitated child abuse and exploitation. Self-regulation in this sense refers to the active responsibility of businesses to counter the negative effects of their products and services, although the term continues to attract divergence of views. Options for self-regulation range from a formal delegation of regulatory powers to industry by government, to self-initiated, organized, and managed "regulation" by industry and other private sector players.[306] Canadian policy experts have noted that "any attempt to regulate the flow of content on the Internet at a national level would be immensely expensive, detrimental to the performance of the network, and easily circumvented [...] rendering such regulation impractical, if not technologically unfeasible."[307] The advantages and limits of self-regulation by technology providers has also been described as follows:

> For fast-moving industries like those of ICTs, the less formal processes of self-regulation make it more flexible and therefore less likely to stifle innovation or excessively limit consumer choice. Further, for such a technical business, it is industry that has the best capability to control quality and recognize low standards. It knows the best way to guarantee quality, the efficacy of potential courses of action and the industry has access to information they need for action at the lowest cost. Third, because industry bears the cost of regulation it has incentives to keep enforcement and compliance costs down.[308]

Self-regulation may not always, however, be a complete solution in itself when it comes to the prevention of ICT-facilitated child abuse and exploitation. Not all social media sites, for example, necessarily monitor user contents nor strictly enforce rules regarding user minimum age.

[306] A/HRC/12/23. Paragraphs 104-109.

[307] Pierlot, P., 2000. *Self-Regulation of the Internet: A Canadian Perspective*. Available at http://www.isoc.org/inet2000/cdproceedings/8k/8k_2.htm#n11.

[308] Ang, P. H., 2001. "The Role of Self-Regulation of Privacy and the Internet", *Journal of Interactive Advertising* 1:1-9.

ISP regulation and opportunities for self-regulation

As the "gatekeepers" to the Internet, ISPs around the world face ever-increasing pressure to implement reporting requirements and mechanisms, or at least codes of conduct, concerning Internet content and acceptable use. Government policies on the matter vary significantly.[309] In the United States and Australia, for instance, ISPs and domain hosts are required to report any identified child sexual abuse material sites to the police within a reasonable period of time, with non-compliance being a punishable offence. Similarly, in South Africa, ISPs must take affirmative measures to prevent their services from facilitating the sharing of child sexual abuse material. ISPs are additionally obliged to reveal any offending user's name and IP address to law enforcement authorities.

From the industry perspective, some ISP-associations have drafted formal codes of conduct that require members to refrain from knowingly accepting illegal content on their sites, and to expediently remove content when they are alerted to its existence. Larger ISPs may also install dedicated "cyberpatrols" that search for illegal sites. Site hosting providers may place responsibility for monitoring content on users by relying on them to abide by their terms of service, or may actively monitor hosted material. Others provide hotlines for users to report suspicious content.[310] Website operators themselves may attempt to render their sites or parts thereof inaccessible to children, by employing techniques for the identification of a user's age, ranging from self-certification, to requiring credit card numbers to get past a "pay wall" to access any adult material contained on the site. This method of screening can be successful, though many teens have access to credit card numbers and thus can bypass such barriers.

With respect to child sexual abuse material, law enforcement agencies have collaborated with ISPs to use a set of layered warning mechanisms to deter curiosity-driven, novice child sexual abuse material-consumers. Specifically, they have developed a series of splash pages that are displayed when suspicious search terms are entered into search engines, that become more severe the more suspicious the search is. The hope is that these warnings will deter people from experimenting with child sexual abuse material and contact abuse conduct.

Blocking access to child sexual abuse material URLs is another form of ISP self-regulation. Using a list of illegal content, ISPs are able to compare content requested by Internet users and block offending materials. Sophisticated software tools can enable ISPs to more effectively block materials, including material accessed through peer-to-peer file sharing programs, where such communications are carried by the ISP. The European Commission has developed a blocking mechanism for ISPs called the Child Sexual Abuse Anti-Distribution Filter, which is currently used by ISPs in Denmark, Finland, Italy, Malta, Norway and Sweden.[311]

[309] A/HRC/12/23. Paragraphs 61-65; see also generally McIntyre, T. J. *Child Abuse Images and Cleanfeeds: Assessing Internet Blocking Systems*. Available at http://www.academia.edu/771272/Child_Abuse_Images_and_Cleanfeeds_Assessing_Internet_Blocking_Systems.

[310] McIntyre, T.J., 2011.

[311] *Ibid*. P. 7-10.

Figure VIII. INTERPOL access-blocking splash page

Source: INTERPOL.

A further example of a blocking programme is INTERPOL's "worst of" list of child sexual abuse material materials. Focused on eradicating the very worst child sexual abuse material on the Internet, INTERPOL coordinates the compilation of a list of the worst child sexual abuse material on the web. The INTERPOL "worst of" list (now called the IWOL) of domains is produced by the same countries that already produce lists according to their national legislation. Domains with very severe child sexual abuse material are seized and shared and re-checked by at least two different child sexual abuse material specialist police forces or countries before being entered onto the IWOL, which is then distributed to all INTERPOL countries and available for free to ISPs/service providers. The ISPs/service providers can sign an agreement with their local INTERPOL office and use the list in all countries where they conduct business. The list can be automatically downloaded from an INTERPOL server in Lyon, France. The criteria to be added to the INTERPOL list is stricter than most national legislations, such as that the child sexual abuse material contain real children who are younger than 13 years of age.[312]

Leading ICT companies, especially ISPs and social networking businesses, also form and participate in a number of global coalitions with a view to combatting child sexual abuse and exploitation and have become key actors in international cooperation on the issue. The International Center for Missing and Exploited Children's (ICMEC) Technology Coalition, for example, is a voluntary collaboration of nine major Internet companies in a bid to develop and execute plans for technology-based solutions to disrupt and dismantle child exploitation criminal enterprises, for which end coalition members can provide technological expertise and resources for preventative measures, detection and documentation of offences.[313]

Financial coalitions

Supplementing the ICMEC Technology Coalition, the ICMEC Financial Coalition Against Child Pornography is a large scale coalition, bringing together 34 leading banks, credit card companies, electronic payment networks, third-party payments companies and Internet services companies, that focuses on curbing money-flows to child sexual abuse material-ventures and coordination of efforts to eradicate commercial child abuse material.[314] Within the Financial Coalition, the Prevention Working Group identifies best practices to eliminate commercial exchange of child pornography. The coalition also encourages its members to inform

[312] See http://www.interpol.int/Crime-areas/Crimes-against-children/Access-blocking

[313] ICMEC. *Making the World Safer for our Children*. Available at http://www.icmec.org/en_X1/icmec_publications/ICMEC_mech.pdf.

[314] NCMEC. *Financial Coalition Against Child Pornography*. Available at http://www.missingkids.com/FCACP; Choo, K. R., 2009. Pp. 68-69.

their customers ("merchants") about diligently monitoring their transactions for child exploitation crimes. The Working Group directly monitors Internet merchants by approving products being sold and investigating links to merchants' websites in order to verify that no off-the-books products or services are processed through the merchant's account. It also cross-references records from pornography websites with credit card information to identify the use of those credit cards on illegal sites. To accomplish these complex tasks, the group tracks and analyses variations in deposit frequency, transaction volume, average ticket price of each sale transaction, change in level of refunds and chargebacks, refunds to credit cards without any corresponding sales, and lack of merchant activity.[315] One of the most important tasks performed by the coalition is the tracking of the origins of funds eventually used in illegal activities to ultimately enable members to close the accounts identified.

On the regional level, the European Financial Coalition (EFC), comprised of financial institutions, credit card companies, third-party payers and ISPs, is also committed to combating child sexual abuse material in the European region. ICMEC has further expanded the financial coalition model to the Asia and the Pacific region.[316]

Self-monitoring by travel and tourism companies

Action taken in the tourism industry can be divided into measures developed in tourist-sending countries and those undertaken in tourist-receiving countries. These measures promote awareness-raising and sensitization to ensure that both travellers and tourism professionals are aware of the issue and are able to take appropriate action against it.

With respect to tourist-receiving countries, mounting public pressure has resulted in the development of a range of anti-trafficking campaigns by hotels, restaurants, common carriers and other agents in the global tourism industries.[317] For example, ECPAT International has orchestrated the creation of a Code of Conduct for the Protection of Children From Sexual Exploitation in Travel and Tourism ("The Code"), which requires participants to undertake the following six steps to help combat child sexual abuse and exploitation in this context: (1) to establish a policy and procedures against sexual exploitation of children; (2) to train employees in children's rights, the prevention of sexual exploitation and how to report suspected cases; (3) to include a clause in contracts throughout the value chain stating a common repudiation and zero tolerance policy of sexual exploitation of children; (4) to provide information to travelers on children's rights, the prevention of sexual exploitation of children and how to report suspected cases; (5) to support, collaborate and engage stakeholders in the prevention of sexual exploitation of children and (6) to report annually on their implementation of Code related activities.[318]

Additionally, in 2006, many travel and tourism companies agreed to abide by the Athens Ethical Principles to End Human Trafficking along with an implementation guide. Participants have agreed to abide by seven principles: (1) to demonstrate the position of zero tolerance towards trafficking in human beings, especially women and children for sexual exploitation; (2) to contribute to prevention of trafficking in human beings including awareness-raising campaigns and education; (3) to develop a corporate strategy for an anti-trafficking policy which will permeate all our activities; (4) to ensure that personnel fully comply with our anti-trafficking policy; (5) to encourage business partners, including suppliers, to apply ethical principles against human trafficking; (6) to call on government as necessary to initiate a process of revision of laws and regulations that are directly or indirectly related to enhancing anti-trafficking policies; and (7) to report and share information on best practices.[319]

Civil society responses

Parents, guardians, child educators and civil society are a vital component in combating ICT-facilitated abuse and exploitation of children, including in supporting children in understanding and handling online risks, the "flagging" of certain material online, the creation of telephone hotlines for reporting, and contributions towards education and psychosocial methods of prevention.

As society has become aware of the vulnerability of children in using ICTs, online safety guides have been developed by the private sector, especially ISPs; governments and

[315] Choo, K. R., 2009. Pp. 68-69.

[316] ICMEC. *Global Efforts to Expand the Financial Coalition*. Available at http://www.icmec.org/missingkids/servlet/PageServlet?LanguageCountry=en_X1&PageId=4355.

[317] See Latonero, M., 2011. P. 35.

[318] http://www.thecode.org/about/.

[319] End Human Trafficking Now. The Athens Ethical Principles. Available at http://www.endhumantraffickingnow.com/?page_id=77.

schools; media sources, such as online newspapers; and NGOs. These guides help parents decide the right age for children to go online, the most appropriate websites for children to visit, the best place for a computer in one's home, and provide information on tools for monitoring and limiting access, as well as discussion points for initiating dialogue with children regarding online behaviour and safety. The need for the active involvement of parents or guardians in children's use of the Internet and other ICTs, supported by adequate access to information, is a key priority identified by such material. In particular, open and frequent dialogue about expectations and actions to take if children encounter something or someone troubling online, is commonly viewed as one of the key steps towards the prevention of ICT-facilitated abuse and exploitation of children.

Parental controls

Filtering tools enable users to block categories of unwanted online content. While some States filter out content perceived as harmful on a national level, others allow customers to control and restrict access to certain content or block search results either at the ISP level, home Internet connection level, or personal computer or device level.

Uniform protocols on filtering have not yet emerged and filters may show significant differences in content blocked, depending upon either the source of block lists used or risk algorithms employed.

Keystroke recording software, as well as device management software, can further enable parents to record all content entered into the family computer through the keyboard, or view lists of URLs visited. Similar protective measures area also increasingly available for smartphones, with some models containing built-in mobile parental control options.

User monitoring or "flagging"

As users of technology, individual members of civil society have assumed a significant role in monitoring and alerting authorities about potential child exploitation offences. In its simplest form, users may "flag" material for follow-up investigation by civilian evaluators or law enforcement agents. Social media sites can enable users to flag inappropriate content uploaded by other users, which is then evaluated by designated employees within the social media company. Content that multiple users have flagged is usually prioritized in this process. As terms of service usually enable service providers to unilaterally take down objectionable content, service providers may simply remove offending content from view. New "panic" buttons also appear on many child-oriented websites and software programmes, such as the latest version of Windows Live Messenger, which enable children to report illicit content or sexual solicitation that they encounter when using these applications.[320] While ideally protecting children from exposure to harmful content, these alarms also provide a mechanism for children to report suspicious content to authorities in an expedient and private way.

One review of twelve popular social media sites found that all of them had a process in place for reporting criminal content to law enforcement authorities. While a useful tool, experts have suggested that flagging represents only a partial solution.[321]

Hotlines

Centralized means for reporting, or "hotlines", are an important and increasingly common and flexible means for law enforcement to generate investigative leads. Hotlines leverage the millions of ICT users who may potentially come into contact with probable child exploitation offences. By providing an efficient and anonymous means for people to report suspicious activity and content, hotlines can serve as a focal reporting point for content such as child sexual abuse material. Good practices for child exploitation hotlines include several elements: clear and efficient communication;[322] clearly defined goals and procedures;[323] meetings and briefings to review results; procedures for identifying and solving problems in closed groups;[324] and methods of continuously revising and improving procedures.[325] Many hotlines also work closely with industry to facilitate "notice and take down" processes, so that content can be removed expeditiously at source.[326]

One example of a hotline, is the Online Child Sexual Abuse Reporting Portal (OCSARP) developed by the Internet Watch Foundation (IWF). OCSARP enables users to report suspected online child sexual abuse images and videos for assessment by IWF analysts. It can be deployed by countries without a hotline as a cost-effective solution that is easy to

[320] A/HRC/12/23; see also Latonero, M., 2011. Pp. 32-33.

[321] FAIR Fund. *Best Practices Guide to Prevent Child Exploitation and Trafficking Online*. Available at http://www.prostitutionresearch.com/pdfs/BestPracticesGuideExploitationChildTraffickingFinal.pdf.

[322] Groupe Speciale Mobile Association (GSMA), 2010. Hotlines: Responding to Reports of Illegal Online Content. (2010).

[323] *Ibid.*

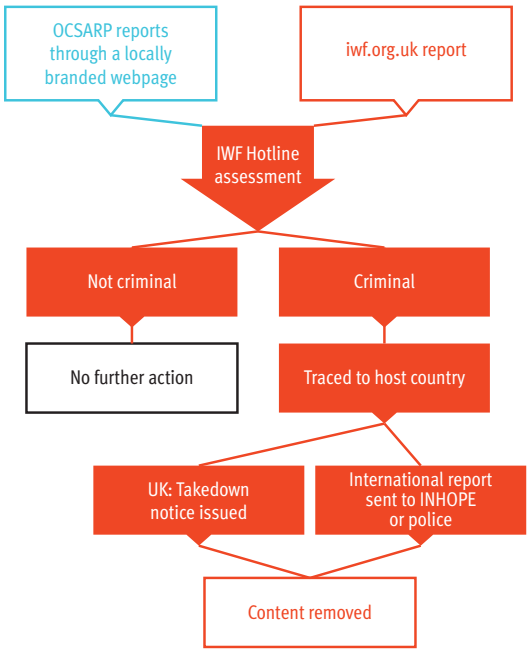
[324] *Ibid.*

[325] *Ibid.*

[326] Expert comments from GSMA Mobile Alliance, April 2014.

implement with back-up support from experts in the field. OCSARP processed 51,186 reports last year.[327] Brazil has operated its own SaferNet hotline since 2005[328] and in the United States, NCMEC's CyberTipline serves as a focal point for receiving reports.[329] Although these hotlines are each focused on a specific country, they cooperate with both domestic as well as international law enforcement.[330] To enhance the impact of the hotline model, the International Association of Internet Hotlines (INHOPE) is an active and collaborative network of 49 hotlines in 43 countries worldwide, committed to eradicating child sexual abuse from the Internet by supporting and enhancing the performance of participating hotlines with the aim of ensuring that swift action is taken in responding to reports of illegal content.[331] In the case of Europe, the European Network of Hotlines coordinates various hotlines that receive reports of child exploitation.

Figure IX. Hotline report processing



A simple flow diagram to show how child sexual abuse images and videos are assessed and removed through OCSARP.

Source: Internet Watch Foundation.

[327] IWF, 2013. P. 10.
[328] See http://www.safernet.org.br/site/.
[329] See http://www.missingkids.com/cybertipline/.
[330] See IWF, 2011. Annual and Charity Report. P. 7.
[331] http://www.inhope.org/gns/home.aspx .

Use of "apps"

A possible emerging area in which civil society can engage to prevent and combat ICT-facilitated child abuse and exploitation lies in the use of mobile "apps" or software applications. To date, few apps exist to protect children from exploitation. However, in June 2011, a coalition of the United States. Agency for International Development and two anti-trafficking NGOs funded a contest for the development of an innovative mobile app to address human trafficking in another country. The winning app used GPS technology to identify and plot on a map nearby places and resources where victims or potential victims could receive help or make reports.[332] Further investment and research on apps to address child exploitation offences would likely yield significant benefits as mobile computing continues to expand.

Education and psychosocial methods of prevention

Education and psychosocial methods of prevention are acknowledged as essential in protecting children from ICT-facilitated abuse and exploitation. Education initiatives enable children, families and other caregivers to understand and rightly assess the risks associated with ICTs. A number of such education, awareness and information programmes exist.[333] The Government of Egypt, for example, in collaboration with technology companies and NGOs, has created and published material aimed at promoting safe use of the Internet by children. Similarly, the European Commission has developed a comprehensive programme called Safer Internet Plus[334] to educate families on a sustained basis, while the Insafe-network operates 26 national awareness centres in Europe.[335] In Peru, municipal Internet squads monitor public areas with Internet access and assist with installation of filters to protect children.[336] Kenyan advocates have formed clubs to promote Internet safety, specially addressing and informing families on ways and means of protecting their children themselves. Other countries rely on peer- and buddy-support systems.[337] Most importantly, however, the consistent

[332] Latonero, M., 2011. P. 33.
[333] A/HRC/12/23. Paragraph 94.
[334] *Ibid*. Paragraph 98.
[335] *Ibid*. Paragraph 95-97.
[336] *Ibid*. Paragraph 99.
[337] ECPAT 2005. *ECPAT International Round Table Meeting on Violence against Children in Cyberspace,Discussion*, Bangkok, Thailand, 12-13 June 2005.

engagement of responsible caregivers in the lives of children is widely recognized as a crucial factor.[338]

Opportunities to enhance the fight against ICT-facilitated child abuse and exploitation

Balancing child protection with human rights

One of the most challenging issues that governments face in preventing and combating ICT-facilitated child abuse and exploitation is that of establishing an equitable balance between child online safety and the safeguarding of internationally recognized human rights.

As the Cybercrime Study notes, computer content-related crimes, such as the ones discussed in the current study, may engage treaty-based rights such as the right to freedom of expression and the positive obligations of states to ensure security of the person and protection from physical harm. Content available on the Internet is, in principle, subject to the same human rights regime as traditional media, such as printed matter and speech.[339] Resolution 20/8 of the United Nations Human Rights Council affirms "that the same rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one's choice".[340]

Nonetheless, online content has particular features—including the fact that the impact and longevity of information can be multiplied when placed on the Internet, that content is easily accessible to minors, and that developments in social media and user-generated Internet content have begun to challenge traditional monopolies over information. As a result, the interpretation of human rights provisions must take into account the specific nature of the Internet as a means of imparting information.[341]

The United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, identifies four forms of expression that are required to be prohibited by international law: child pornography; direct and public incitement to commit genocide; advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence; and incitement to terrorism.[342]

Thus, whereas the human rights position on the prohibition of child sexual abuse material is clear, restrictions on some other forms of content and acts discussed in this study, such as "sexting", or locating publicly available information on an individual, is significantly less clear from a human rights perspective. As governments seek to develop effective responses to the whole range of forms of ICT-facilitated abuse and exploitation, it is important that they do so in full conformity with international human rights standards—both as they relate to victims and perpetrators.

In this respect, one starting point is the development of international consensus in the form of international "block" lists, standards, and policy recommendations, where available. Industry associations can a play role in promoting and achieving such consensus. Operator members of the GSMA Mobile Alliance against Child Sexual Abuse Content, for example, commit to implementing blocks on lists of child sexual abuse material URLs only as defined by credible third parties—including the IWF CAIC list[343] and the INTERPOL "worst of" list. The GSMA's role in this area is to promote this approach as a good practice by, for instance, facilitating new members' access to the lists by brokering relationships with the IWF and/or INTERPOL, sharing toolkits on implementation, and advocating for clear legislative frameworks where necessary.

Ensuring that legislation keeps pace with technological innovation

A further challenge encountered by governments consists of enacting laws that keep pace with advances in technology. Many States have updated their computer-crime laws to address innovations in ICTs. In order to have a lasting and sustained effect, however, revisions to existing laws and new laws must be drafted in a flexible way and in a "technology-neutral" manner, so as to keep up with technological innovation without needing constant reform. Laws and international

[338] Commentary at the Informal Expert Group Meeting on the Effects of Information and Communication Technologies on the Abuse and Exploitation of Children. Vienna, 23-26 September 2013.

[339] See UNODC, 2013. Pp. 107-116.

[340] United Nations Human Rights Council, 2012. Resolution 20/8 on The promotion, protection and enjoyment of human rights on the Internet [A/HRC/RES/20/8].

[341] UNODC, 2013. P. 109.

[342] See United Nations General Assembly, 2011. *Promotion and protection of the right to freedom of opinion and expression. Note by the Secretary-General* [A/66/290].

[343] https://www.iwf.org.uk/members/member-policies/url-list/testing-policy

cooperation mechanisms must also address the need for timely access to information across national boundaries. Finally, legislators themselves must receive sufficient training and guidance on making sound decisions in the formulation of effective laws.

Establishing specialized units with dedicated personnel

Specially trained and dedicated personnel with relevant skills are crucial in combatting ICT-facilitated child abuse and exploitation. The Cybercrime Study noted that less than one per cent of all police are specialists in cybercrime.[344] In turn, only a part of that percentage may be specially trained and dedicated to investigating the use of ICTs in child exploitation offences. Consequently, many child exploitation investigations may not involve digital forensic examiners and the expertise these could bring to the investigations.

Investigators specialized in child abuse and exploitation tend to be more effective in collecting evidence from physical crime scenes. For instance, in addition to searching for child sexual abuse material, such as evidence on computers and related technology, specialized investigators may also search the offender's home more effectively for other related evidence, such as toys or items used to subdue child victims. Such evidence could strengthen and support digital evidence against a suspect. When and where specialized and dedicated units exist, members should also receive training on interviewing child victims and witnesses, including topics such as how to use age-appropriate settings for interviews, and the use of dolls and drawings to elicit details from young children with limited vocabularies.

Experienced and dedicated personnel also tend to develop transnational networks of contacts that work on child exploitation issues. Resulting relationships may facilitate cooperation on an informal basis in preparation for subsequent transnational investigations.[345]

Additionally, specialized personnel can also better identify and respond to common defences employed by suspects during judicial proceedings, such as claims that "someone else did it" using their equipment, that contraband material was downloaded by mistake, or that the perpetrator was unaware that the victim was a minor.

At trial stage, ICT-specialized prosecutors are able to more clearly and persuasively present technical evidence to judges and juries. They may, for example, develop skills in structuring the order of witnesses called and in organizing the conduct of witness examination to present technical evidence at a digestible rate.

Accessing state-of-the-art technological resources

In order to keep pace with technological innovation and effectively combat child exploitation, investigators require access to state-of-the-art equipment. Cutting-edge technology devices and software, including high-quality equipment for storing and processing data, enable investigators to operate the equipment that many criminals use in perpetrating child abuse and exploitation crimes.[346] Continuous training on new tools and emerging technologies are also imperative.

As the costs of technology decrease, offenders can amass ever greater data-storage capacities. As a result, investigators may increasingly require access to sophisticated case management software. In 2002, for example, Microsoft developed the Child Exploitation Tracking System (CETS) to help law enforcement agencies efficiently track hundreds of suspects at once, follow up on leads, and collect evidence against suspected child sexual abuse material offenders.[347] However, in many countries, investigators have neither the training nor the equipment necessary to operate CETS or similar tools.

Law enforcement agencies must also decide on how to best allocate scarce technological, financial and skilled human resources.[348] While consensus exists on the importance of protecting children from online offenders, law enforcement agencies may face other resource claims with high priority, including terrorism, gangs, and organized crime activities.

Access to third-party data and other evidentiary challenges

In a cloud and remote server-based web environment, investigators are increasingly required to collect evidence from third parties, such as Internet service providers, mobile telephone

[344] UNODC. 2013. P.154.

[345] Interview with Michael Moran, Chief Investigator, Crimes Against Children Unit, INTERPOL, 14 March 2012.

[346] Offenders may use larger quantities of data due to the decrease in price of external storage devices and additional virtual storage capacity available in cloud environments.

[347] Harmon, B., 2012. *Microsoft PhotoDNA Technology to Help Law Enforcement Fight Child Pornography*, 19 March 2012. Available at http://blogs.technet.com/b/microsoft_on_the_issues/archive/2012/03/19/microsoft-photodna-technology-to-help-law-enforcement-fight-child-pornography.aspx.

[348] See Etter, B., 2003.

companies, social media and photo sharing businesses and other third-party providers. Ordinarily, third parties delete data after a certain period in order to clear server space for further use.[349] The Cybercrime Study noted that the interplay between law enforcement and service providers is particularly complex. National legal obligations and private sector data retention and disclosure polices vary widely by country, industry and type of data. Service providers most commonly require due legal process for disclosure of customer data. Accordingly, in many jurisdictions, a court order must be obtained in order to access electronic evidence from service providers. In some cases, law enforcement may be able to obtain data directly, especially where this is facilitated by informal partnerships between law enforcement authorities and service providers.

As an increasing number of crimes, including forms of child abuse and exploitation, involve digital evidence held by third parties, it is critical that industry and governments work together to develop mechanisms for timely law enforcement access to data in emergency situations, combined with fair and transparent legal processes for routine investigations.

Establishing the means to conduct undercover investigations

ICT-facilitated abuse and exploitation offences commonly require undercover operations. Accordingly, first and foremost, States need a clear legal framework for undercover or covert operations that takes full account of human rights and rule of law standards.[350] Many offenders may require their victims or co-perpetrators to engage in initiation rites, such as the upload of child sexual abuse material, in order to dissuade undercover law enforcement agents. Policies and laws must exist that clearly set out protections and liabilities for law enforcement officers who encounter such situations.

Undercover operations are most useful where States have clear criminalization provisions for inchoate crimes, such as attempts or preparation for an offence. In the absence of such legal provisions, investigators cannot arrest would-be offenders until and unless the crime is completed, such as when the victim is actually abused or exploited. This situation, in turn, considerably undermines the purpose of anti-child abuse and exploitation laws, policies and operations.[351]

Increasing awareness and knowledge of the issues

Non-governmental organizations and members of civil society face the challenge of building upon the public's general, although sometimes vague, perception of and awareness of the risks that have been created by ICTs in the context of child sexual abuse and exploitation. Particularly in regions of the world that have limited and only fairly recent access to ICTs and are not yet sufficiently familiar with the associated risks and hazards, parents and guardians often lack the specific awareness and skills to protect their children. Even where broad and relatively sophisticated awareness has been built, NGOs and members of civil society must continue to raise awareness on and highlight specific risks and appropriate counter-measures. [352]

Contemporary awareness programmes are likely to have to undertake concerted efforts to overcome both saturation regarding digital safety warnings, as well as false confidence on the part of children and parents about how up-to-date their level of online safety knowledge is. One emerging idea in the field of awareness-raising is the concept of "digital citizenship", which relates to the norms of appropriate, responsible technology use and addresses the topics of digital access, commerce, communication, literacy, etiquette, law, rights and responsibilities, health and wellness and security.[353]

Addressing research gaps

The research community faces the considerable challenge of filling in the many gaps that exist and continue to emerge in knowledge on ICT-related child sexual abuse and exploitation. These include up-to-date victimological studies regarding which children may be most susceptible to harm, research on victimology and perpetrator-profiles with regard to the developing world, as well as the trend towards increasing levels of violence and increasingly younger victims depicted in child sexual abuse material.

[349] For a review of typical data retention times, see UNODC. 2013. P.147-148.

[350] Bose, A., 2013.

[351] Wei, W., 2010. *Online Child Sexual Abuse Content: The Development of a Comprehensive, Transferable International Internet Notice and Takedown System*. Available at https://www.iwf.org.uk/assets/media/resources/IWF%20Research%20Report_%20Development%20of%20an%20international%20Internet%20notice%20and%20takedown%20system.pdf.

[352] UNICEF, 2011. Pp. 7-9, 21.

[353] https://www.iste.org/;http://www.digitalcitizenship.net/

Research on the interdependencies between society's perceived risks and actual harms would be especially valuable for policymakers faced with the difficult task of allocating scarce resources. Along similar lines, research on the ways in which certain intrinsic and extrinsic factors affect children's vulnerability to abuse and exploitation would also be of use in evidence-based policymaking.[354]

Equally, research on offender profiles is also needed. Of particular interest in this regard is the relationship between contact and non-contact abusers, and an understanding of the causal impact that contact and non-contact abuse have on each other.

Research on the demand side is also essential in order to prevent commercial sexual abuse and exploitation of children. For instance, some regions of the United States have experimented with extended education programmes for first-time prostitution offenders.[355] Likewise, several European countries are pioneering various programmes to deter commercial sexual exploitation of children.[356] With respect to child sex abuse and exploitation in the travel and tourism industries, various education campaigns have been initiated to curb demand. For example, NGOs have executed multimedia campaigns to deter sex tourists at places in airports, in-flight videos, tourist magazines, and billboards in tourist areas.[357]

Developing policy guidance on harmful conduct committed by youth

With regard to cyberbullying, recent successful policies have aimed at informing, training and supporting parents, teachers and children in coping with such conduct and working with perpetrators, especially child bullies. With respect to exposure to harmful content, attention has focused on educating parents about the hazards associated with video games, social media sites and mobile apps, and the need for parents to profoundly and personally engage with their children in order to effectively protect them.

One of the most challenging issues in the formation of policy is the issue of child exploitation offences committed by other youth. Some crimes such as cyberenticement by definition involve an adult offender and a minor victim. However, other child sexual abuse material offences, commercial sexual exploitation of children, cyberstalking and cyberbullying, and exposing children to harmful content can be executed by minors. In some child-on-child offences, the youth perpetrating the harmful conduct acts much such as an adult offender. For example, children who engage other children in commercial sexual exploitation are creating harm that is not likely to be mitigated by the young age of the perpetrator. In other cases, the impact of peer-on-peer conduct such as sexting is less clear. Such newly emerging trends and phenomena need to be better understood through qualitative and quantitative research, with a view to producing clear policy guidance.

States also have a strong interest in treating young offenders differently from adult offenders, in particular when it comes to applying mandatory minimum sentences or to being registered as a sex offender. In charting a path on this issue, policymakers should consider whether or not the nature of the act itself and the harm arising from it, both for the victim and society at large, is altered by the fact that the offence in question was committed by a minor. In formulating such policies, a multidisciplinary approach that draws on research findings and best practices from social science, legal policy and public policy is highly advisable.

Mitigating negative effects by the private sector

Many private sector businesses and technology companies are motivated by a strong sense of corporate social responsibility and a desire to comply with internationally recognized human rights standards. Such standards can also apply to investment in combatting ICT-facilitated child abuse and exploitation, and the links between social responsibility, human rights, and child protection should be increasingly emphasized.

---

[354] Bose, A., 2013.

[355] See Shively, M., et al., 2008. , Final Report on the Evaluation of the First Offender Prostitution Program. Available at https://www.ncjrs.gov/pdffiles1/nij/grants/221894.pdf.

[356] See Scoular, J., 2004. "Criminalising 'Punters': Evaluating the Swedish Position on Prostitution", *Journal of Social Welfare and Family Law*, 26:195-210; Marinova, N. K., James, P., 2012. "The Tragedy of Human Trafficking: Competing Theories and Evidence", *Foreign Policy Analysis* 8:231-253.

[357] World Vision. World Vision's Work on Sex Tourism to Prevent Sex Tourism. Available at http://www.worldvision.org/worldvision/pr.nsf/stable/child_sex_tourism_wvwork.

GLOSSARY

Application software (app)	A computer program designed to carry out a specialized task or tasks for the user, such as database management, word processing or electronic mail. A mobile app is software designed to run on mobile devices.
Banner advertising	A popular form of website advertising utilizing a rectangular graphic display that stretches across the top or bottom of a website or down the right or left sidebar and when clicked on, directs the user to the website of the advertiser.
Child sex tourism/ travelling child abusers	Child sex tourism is a form of commercial sexual exploitation of children by men or women who travel from one place to another, and there engage in sexual acts with children.
Cyberbullying	The use of ICTs to harm a victim or victims in deliberate, repeated and hostile ways and eased by the apparent anonymity and distance from the victim.
Cyberharassment	The use of ICTs to intimidate, repeatedly or otherwise, one individual by another or by a group.
Cyberstalking	The use of ICTs to undertake activities related to locating, surveying, harassing or manipulating victims that causes distress, fear or alarm, being mainly characterized by the repetitive aspect of the conduct.
Cyberenticement	The use of a computer or similar device to contact a person who is or is believed to be a minor to solicit, encourage, entice, or lure him or her for the purposes of engaging in sexual activity in violation of the law.
Dark net	Part of the deep web in which both web users and website publishers are largely anonymous due to obfuscation technology.
Deep web	All parts of the Internet which cannot be indexed by search engines.
Download	An act of moving or copying a file, program, etc. from a usually larger computer system to another computer or device.
Filter	Software for sorting or blocking access to certain online material.
Geotag	A piece of data embedded in a digital media file to indicate geographical information.
Global positioning system (GPS)	A navigational system using satellite signals to fix the location of a radio receiver on or above the earth's surface.
Instant messaging	A means or system for transmitting electronic messages in near real time.
Internet protocol address (IP address)	A number that uniquely identifies each host using the Internet.

Internet service provider (ISP)	An enterprise that provides services for accessing, using or participating in the Internet.
Online grooming	The use of ICTs to undertake a process by which a person prepares a child, significant adults, and the environment for the abuse of the child. Specific goals include gaining access to the child, gaining the child's compliance and maintaining the child's secrecy to avoid disclosure.
Online solicitation	The use of ICTs by an adult to propose to meet a child who has not reached the legal age of consent for the purpose of engaging in sexual activities or the production of child sexual abuse material.
Peer-to-peer file sharing	The distribution and sharing of digital documents and computer files directly between Internet connected devices using a specialized software program that searches for other connected computers on a network and locates the desired resource.
Sexting	The sending of a form of self-generated sexually explicit messages or images through mobile phones and/or the Internet and typically involves minors.
Short Message System (SMS)/text message	A short message that is sent electronically usually from one cell phone to another.
Smartphone	A device that combines a mobile phone with a hand-held computer, typically offering Internet access, data storage, e-mail capability, among other things.
Social media	Forms of electronic communication through which users create online communities to share information, ideas, personal messages and other content.
Social networking service	Online utilities that enable users to create profiles, public or private, and form a network of friends. Social networking services allow users to interact with friends via private and public means, such as messages and instant messaging, and to post user-generated content, such as photos and videos. Examples of social networking services include Facebook, Mxit and Orkut.
Tor	Tor (The Onion Router) refers to a network of virtual tunnels that allows people and groups to improve their privacy and security on the Internet. It also enables software developers to create new communication tools with built-in privacy features.
Universal Resource Locator (URL)	A web page's unique location or address on the Internet.
Web browser	Software that enables users to locate, access and view web pages (e.g. Internet Explorer, Google Chrome, Mozilla Firefox).

UNODC

United Nations Office on Drugs and Crime

Vienna International Centre, P.O. Box 500, 1400 Vienna, Austria
Tel.: (+43-1) 26060-0, Fax: (+43-1) 26060-5866, www.unodc.org

V.14-08450