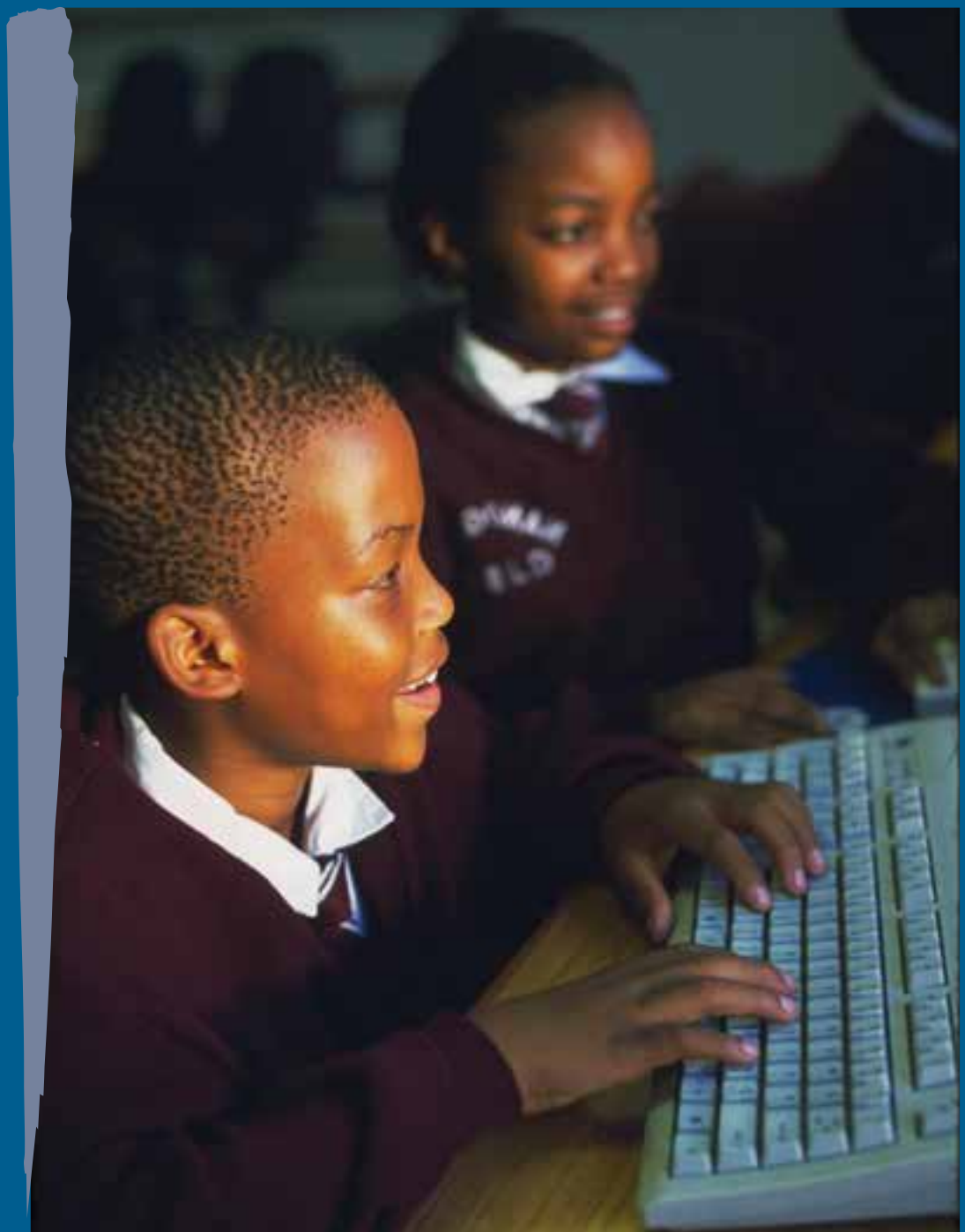
OFFICE OF THE SPECIAL REPRESENTATIVE OF THE SECRETARY-GENERAL ON
VIOLENCE AGAINST CHILDREN

Releasing children's potential and minimizing risks

ICTs, the Internet and violence against children



Releasing children's potential and minimizing risks

ICTs, the Internet and violence against children

Publication produced by the Office of the SRSG on Violence against Children in 2014

Cover photo: © UNICEF/NYHQ200-0206/Pirozzi

In 2001 in Botswana, two children work at a computer terminal in a junior secondary school in Gaborone, the capital.

e-ISBN: 978-92-1-058284-1

Printing: UNON, Publishing Services Section/Nairobi, ISO 14001:2004-Certified

Contents

A Click Away (Todo a 1 Clic)

1. When we use technologies we are a click away from producing positive situations and avoiding bad ones.
2. We recognize that we all have rights and responsibilities when we interact.
3. We request States and the private sector to promote the use of the Internet for all adolescents.
4. The way in which we connect using technologies is a personal choice, and we undertake to do this without causing harm to others.

The *Todo a 1 Clic* manifesto was developed by more than 1,000 teenagers from seven Latin American countries during national forums and a regional online awareness-raising campaign. During the first phase of this project, in May 2014, young people set out the four points listed above.

The Todo a 1 Clic initiative has been developed by RedNATIC, coordinated by Asociación Chicos.net (Argentina) and Fundación Paniamor (Costa Rica), with the support of Google and Save the Children.

© UNICEF/MENA03601/Pirozzi

Glossary

App: Abbreviation of 'application'—a programme or piece of software developed for a specific purpose. A mobile app is designed to run on smartphones, tablet computers and other mobile devices.

Blog: A website with entries, or 'posts' including text and images, typically displayed in chronological order.[1]

Broadband: A high-capacity digital connection that facilitates a faster Internet connection and enables a more rapid exchange of larger files such as videos, games and software applications.[2]

Chat room: A virtual 'meeting room' where individuals communicate by typing messages ('chatting') to each other in real time. Most chat rooms focus on a particular topic or theme.[3]

Child pornography: Under the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography, child pornography is defined as "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". To avoid child victims' stigmatization, the 2008 Rio de Janeiro Declaration and Call for Action to Prevent and Stop Sexual Exploitation of Children and Adolescents uses the term "child abuse images" and the expression 'child sexual abuse images' or 'child sexual abuse material' is being increasingly used by child rights experts, law enforcement agencies and academics.

Cyberbullying: Any aggressive, intentional act carried out by a group or individual, using electronic forms of contact, against a victim who cannot easily defend himself or herself. Typically, cyberbullying is carried out repeatedly and over time, and is characterized by an imbalance of power.[4]

Cybercrime: Any criminal act committed via the Internet or another computer network, including theft of banking information or personal data, production and dissemination of illegal material, online predatory crimes and unauthorized computer access.

Cyberstalking: Repeated harassment of a victim by a person or persons using the Internet or other electronic means.

Deep Web: Content on the World Wide Web that is not part of the 'Surface Web'—i.e. not part of the Web that can be indexed by search engines.

Email: Abbreviation of 'electronic mail', a tool that allows for exchange of messages between electronic mailboxes over a communications network such as the Internet.[5]

File sharing: The transmission of files—including computer programmes, documents and multimedia material—from one computer to another, over the Internet or a network.

Filter: A mechanism to sift out and block access to certain material. The programme may be designed to operate on a personal computer or may be applied to a network of computers.[6]

Grooming: Online contact with children that includes premeditated behaviour intended to secure their trust and cooperation prior to engaging in sexual conduct.[7] Grooming is characterized by a clear power imbalance between the perpetrator and the victim or victims.

Hacker: Commonly understood as an individual who exploits weaknesses in a computer system or network to gain unauthorized access to data.

---

1 UNICEF, *Child Safety Online: Global challenges and strategies*, UNICEF, 2011, pp 31-32.

2 Ibid.

3 Ibid.

4 Slonje, Robert, Peter K. Smith and Ann Frisén, 'The nature of cyberbullying, and strategies for prevention', *Computers in Human Behavior*, 2012, retrieved 20 June 2014 from <http://dx.doi.org/10.1016/j.chb.2012.05.024>.

5 UNICEF, op. cit.

6 Ibid.

7 Choo, Kim-Kwang Raymond, 'Online Child Grooming: A literature review on the misuse of social networking sites for grooming children for sexual offences', Australian Institute of Criminology, AIC Reports, Research and Public Policy Series, no. 103, 2009, p. x.

Associated with malicious programming attacks on the Internet.

Information and communication technologies (ICTs): An umbrella term that includes any information and communication device or application and its content. This definition encompasses a wide range of access technologies, such as radio, television, satellites, mobile phones, fixed lines, computers, network hardware and software.[8]

Instant messaging (IM): A text-based communication service, normally relying on a 'friends' list predetermined by the user. Most social networking sites have an IM function.[9]

Internet: Worldwide network of interconnected computer networks, using a common set of communication protocols and sharing a common addressing scheme. The Internet facilitates the transmission of email messages, text files, images and many other types of information among computers.[10]

Internet service provider (ISP): A commercial enterprise that provides users with access to the Internet, usually for a fee, or a business that provides Internet services such as website hosting or development.[11]

Live streaming: Live (video or audio) content delivery over the Internet, from a provider to an end user.

Microblog: Any social media site to which users upload brief, frequent posts. Twitter is currently a leading microblogging service

Peer-to-peer (P2P): Software that allows transmission of data directly from one computer to another over the Internet, usually without needing to involve a third-party server.[12]

Phishing: A fraudulent attempt to acquire sensitive information, such as passwords, credit card details or bank account information by presenting an apparently legitimate request in an electronic communication (especially emails, instant messaging or phone calls).

Photo sharing: An application that enables users to upload, view and share photographs.[13]

Sexting: A form of messaging or texting in which people send self-generated pictures of a sexual nature or sexually explicit texts.[14]

Sextortion: Non-physical coercion of an individual with a view to obtaining money or sexual favours or material. Perpetrators of sextortion often threaten victims with the dissemination of compromising photographs.

Short message service (SMS): A text messaging service available on mobile phones, other handheld devices and computers.[15]

Smartphone: Mobile phones that incorporate a complete operating system and are able to access the Internet.[16]

Social media: Primarily Internet- and mobile-based tools for sharing and discussing information. Social media most often refers to activities that integrate technology, telecommunications and social interaction and are used to share words, pictures, video and audio.[17]

Social networking sites: Online utilities that enable users to create (public or private) profiles and form a network of friends. Social networking sites allow users to interact with friends via public or private means, such as messaging and instant messaging, and to post user-generated content.[18]

Spam: Indiscriminate unsolicited electronic messaging sent in bulk, especially advertising material.

Text messaging/texting: Short text messages sent using mobile phones and wireless handheld devices.[19]

Video sharing: An application that allows users to upload, view and share videos.[20]

---

8 Broadband Commission for Digital Development, Global Initiative for Inclusive Information and Communication Technologies (G3ict), The International Disability Alliance, ITU, Microsoft, Telecentre.org Foundation and UNESCO, *The ICT Opportunity for a Disability-Inclusive Development Framework*, ITU, 2013, p. 6.

9 UNICEF, op. cit.

10 Ibid.

11 Ibid.

12 Ibid.

13 Ibid.

14 Ibid.

15 Ibid.

16 Ibid.

17 Ibid.

18 Ibid.

19 Ibid.

20 Ibid.

1. Introduction

Information and communication technologies (ICTs) are developing ever more rapidly, with profound effects upon societies around the world. They bring with them enormous benefits and opportunities, most especially by facilitating access to the Internet. ICTs are creating new ways of communicating, learning, delivering services and doing business.

For children and youth, who are often particularly adept at harnessing the potential of these technologies, ICTs and the Internet represent an important opportunity for empowerment and engagement, offering new means of experiencing creative processes, communication, social interaction, entertainment and learning. Children are not simply passive recipients of information; they are also engaged participants and actors in the online world (see table 1).

In addition to promoting children's empowerment and participation, new technologies are proving to be increasingly useful for ensuring children's protection. They provide opportunities for young people to access information from institutions (including ombudspersons), seek advice from child helplines, report incidents of violence and ask for help when they feel at risk (see box 1).

Table 1.
Online empowerment: children as recipients, participants and actors[21]

	Child as recipient (online content)	Child as participant (online contact)	Child as actor (online conduct)
Education, learning and literacy	Educational resources	Contact with others who share one's interests	Self-initiated or collaborative learning
Participation and civic engagement	Global information	Exchange among interest groups	Concrete forms of civic engagement
Creativity	Diversity of resources	Being invited/inspired to create and participate	User-generated content creation
Identity and social connection	Advice (personal, health, sexual, etc.)	Social networking, shared experience with others	Expression of identity

[21] Livingstone, S. and L. Haddon, *EU Kids Online*, London School of Economics and Political Science (LSE) and EU Kids Online, 2009, p. 8.

Box 1.
Using ICTs to enhance child protection

In Benin, Plan International has been exploring how text messaging (SMS) and the Internet can support reporting of incidents of violence against children and improve both immediate and longer term responses. The pilot has involved raising awareness among young people and training them to create and upload multimedia content about the situation in their area.[22]

Proteja Brasil (Protect Brazil) is an application for smartphones and tablet computers that enables fast and effective reporting of violence against children and adolescents. Based on location, it displays telephone numbers, addresses and the best routes to the nearest police stations, protection councils and other organizations that help to combat violence against children in major Brazilian cities. It also provides information about different forms of violence.[23] The app is part of the Convergence Agenda, a national initiative designed to protect boys and girls from violence during large events, such as the 2014 FIFA World Cup.

A mobile application called MediCapt, designed to help clinicians more effectively collect, document and preserve forensic medical evidence of sexual violence, is being tested in the Democratic Republic of the Congo. Developed by Physicians for Human Rights, this tool converts a standardized medical intake form for forensic documentation to a digital platform and combines it with a secure mobile camera to facilitate forensic photography. MediCapt helps preserve critical forensic medical evidence of mass atrocities, including sexual violence and torture, for use in courts.[24]

In Guatemala, in the context of a Population Council project, girl leaders and members of girls' clubs have been involved in a community mapping exercise. Using GPS technology, they have plotted every household, building and route in their communities to produce maps that show where girls and women feel safe or at risk.

In Uganda, UNICEF launched the uReport initiative in 2010. This involved training Boy Scouts from across the country as social monitors, tasked with reporting directly from their communities via SMS on a range of important issues, including child protection. Conducted regularly, uReport polls can be seen on an Internet-based user interface. In just minutes, UNICEF can identify key child protection issues across the country and identify where disparities are greatest. As this network grows, the data it produces can be used in diverse ways, such as to improve development planning and donors' aid allocation decisions. The data will also empower community members to use the information for advocacy and to hold governments and donors accountable for their promises.[25]

The Internet collapses physical distance and offers a vast, largely unregulated 'space' accessible to all by means of computers, laptops and increasingly mobile devices such as smartphones and tablets.[26] Openness and accessibility are fundamental aspects of the Internet—but therein also lie some of the greatest risks, in particular concerning the safety and well-being of children and young people. ICTs, and the unsupervised online access they facilitate, make children potentially vulnerable to violence, abuse and exploitation in ways that are often difficult for parents, caregiv-

22 Ibid., p. 8.

23 About Protect Brazil' retrieved 6 June 2014 from <www.protejabrasil.com.br/us/>.

24 Physicians for Human Rights, 'MediCapt', retrieved 11 September 2014 from <http://physiciansforhumanrights.org/medicapt/>.

25 Mattila, Mirkka, 'Mobile Technologies for Child Protection, A briefing note', UNICEF WCARO, 2011, pp. 9-10.

26 While the Internet is indeed vast and unregulated, human rights and fundamental freedoms apply equally offline and online. The Committee of Ministers of the Council of Europe underlines that Council of Europe member States have the obligation to secure for everyone within their jurisdiction the human rights and fundamental freedoms enshrined in the European Convention on Human Rights, and notes that, "[t]his obligation is also valid in the context of Internet use." See Recommendation CM/Rec (2014)6 of the Committee of Ministers to member States on a 'Guide to human rights for Internet users' (adopted by the Committee of Ministers on 16 April 2014 at the 1197th meeting of the Ministers' Deputies), §1.

ers, teachers and others to detect and respond to. Furthermore, technological advances have been so rapid that parents and caregivers often struggle to keep up with developments, especially in areas with low levels of digital literacy.

The Internet and ICTs have heightened the potential impact of existing forms of violence, abuse and exploitation. These include:

- Children's exposure to disturbing or potentially harmful content on websites and online forums and blogs;
- Proliferation of child sexual abuse images and materials, and with this, increased levels of harm for the victims and increased levels of profits for criminal enterprises;[27]
- Development of virtual networks of individuals whose principal interest lies in child sexual abuse or child trafficking and other forms of exploitation;
- Inappropriate contact with children and 'grooming' by unknown adults; and
- Cyberbullying, by means of email, online chat services, personal web pages, text messages and other forms of electronic content.

Additional issues include children's exposure to unsolicited or age-inappropriate advertising and online pressure to make purchases or pay for services; overuse of ICTs; and Internet 'addiction', which often results in children's involvement in age-inappropriate gaming or games with high levels of violent, racist or sexist content. Online gaming communities can also be used by paedophiles seeking to make contact with children, or by bullies as a platform for their abusive behaviour.

Other forms of online violence, abuse and exploitation might be considered as new phenomena, such as made-to-order child sexual abuse material; user-generated and self-generated content including sexting; and broadcasting of child sex abuse, often by live streaming.[28]

Finally, evidence is beginning to emerge of children's own involvement in cybercrime, including hacking, online scams and consumption and dissemination of child sexual abuse materials.

Concern about the role of technology in generating and encouraging violence against children has been growing in recent years. As early as October 1996, the United Nations Committee on the Rights of the Child dedicated a day of general discussion to 'The child and the media'. This included reflections both on the role of the media in offering children the opportunity to express their views and on protection of children from information that might have a harmful impact on them, including material depicting "brutal violence and pornography".[29]

In 2006, the United Nations Study on Violence against Children acknowledged that "[t]he Internet and other developments of communication technologies [...] appear to be associated with an increased risk of sexual exploitation of children, as well as other forms of violence."[30] In 2008, 'The Rio de Janeiro Declaration and Call for Action to Prevent and Stop Sexual Exploitation of Children and Adolescents', the outcome document

[27] There is currently a lack of clarity around the terminology employed in the context of child pornography. The term 'child pornography' is used in all relevant international and regional standards and is also found in the domestic legislation of many countries that have harmonized their national laws with the provision of relevant international and regional legal instruments. However, from around 2001, academics, law enforcement agencies and child rights NGOs began to replace 'child pornography' with terms such as child abuse images' and 'child abuse materials'. ECPAT International indicates that the rationale behind this change is based on the concern that the term 'child pornography' may give the impression that a child consented to sexual exploitation and that it does not accurately reflect the abuse suffered by the victim. At present, there is no consensus among stakeholders about which term should be used in place of 'child pornography'.

[28] UN Commission on Crime Prevention and Criminal Justice, 'Study facilitating the identification, description and evaluation of the effects of new information technologies on the abuse and exploitation of children', 7 May 2014, E/CN.15/2014/CRP.1, p. 15.

[29] www.ohchr.org/Documents/HRBodies/CRC/Discussions/Recommendations/Recommendations1996.pdf.

[30] Pinheiro, Paulo Sérgio, 'Report of the independent expert for the United Nations study on violence against children', 29 August 2006, A/61/299, ¶77.

of World Congress III against Sexual Exploitation of Children and Adolescents, expressed concern at "the increase in certain forms of sexual exploitation of children and adolescents, in particular through abuse of the Internet and new and developing technologies [...]."[31]

The International Association of Internet Hotlines (INHOPE) has indicated that online child sexual exploitation is likely to rise in coming years, as Internet adoption rates expand globally and demand increases for new child sexual abuse material. INHOPE and its member hotlines experienced a 14 per cent increase in the number of complaints concerning illegal online content handled globally in 2013, with a dramatic 47 per cent increase in the number of confirmed reports of child sexual abuse material.[32]

The rapid development of ICTs and the reach of the Internet are global phenomena, but this does not mean they are experienced in the same way around the world. Although comparable research and data are not available for all countries and regions, studies suggest that in industrialized countries, awareness of the risks to children associated with the Internet has been increasing. Indeed, the 2013 Global Survey on Violence Against Children, conducted by the Special Representative of the Secretary-General (SRSG) on Violence against Children, notes "a growing awareness of the potential of the Internet and mobile communication devices for awareness-raising and reporting violence, and the efforts of certain States to increase knowledge of the risks associated with the online environment through surveys, research and online campaigns."[33] However, the scenario is different in many lower- and middle-income countries, where "the Internet is growing at breakneck speeds, making it hard to assess how young people are using it, let alone how to protect them from underlying dangers."[34]

Around the world, there are valuable lessons to be learned and shared. In keeping with their international obligations, governments can and to some extent do influence children's online safety. They do so by:

- Introducing appropriate legislation;
- Developing effective policy responses and appropriate monitoring tools;
- Training law enforcement officials, teachers, child protection officers and other professionals working with children;
- Raising awareness of online risks among children and their parents and caregivers;
- Providing counselling and complaint mechanisms;
- Supporting recovery for children who have been exposed to violence, abuse and exploitation;
- Collecting data; and
- Incentivizing the corporate sector to introduce measures to enhance children's online safety.

With a view to promoting the empowerment of children in the online environment and accelerating progress in online protection for children, the SRSG held an international consultation on this issue in June 2014 in San Jose, Costa Rica. Input from the national and international experts who attended this meeting provided important contributions to the present study.

31 'The Rio de Janeiro Declaration and Call for Action to Prevent and Stop Sexual Exploitation of Children and Adolescents', the outcome document of World Congress III against Sexual Exploitation of Children and Adolescents, Rio de Janeiro, Brazil, 25-28 November 2008.

32 INHOPE, 'Online child sexual exploitation likely to rise in the coming years', press release, 16 April 2014, retrieved 22 May 2014 from <http://inhope.pr.co/74794-online-child-sexual-exploitation-likely-to-rise-in-the-coming-years>.

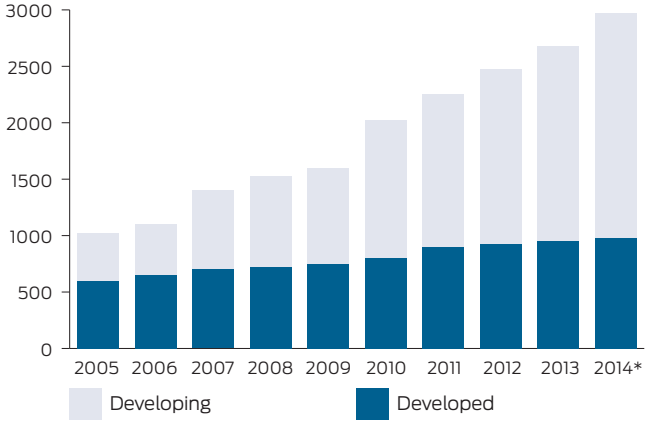
33 SRSG on Violence against Children, *Toward a World without Violence. A global survey of violence against children*, Office of the SRSG on Violence against Children, 2013, p. 133.

34 Elder, James, 'New UNICEF report examines the risks facing children online', 2011, retrieved 25 October 2013 from <www.unicef.org/protection/57929_60984.html>.

2. The global reach of ICTs and the Internet

The reach of the Internet increases every year. Indeed, the rapidity of change in the field of information technology means that statistics have a short shelf life. At the beginning of 1998, less than 200 million people around the world were online. By the end of 2011, this figure had risen to 2.3 billion,[35] and by the end of 2014 the number of Internet users globally is expected to have reached almost 3 billion (figure 1). Of these, two thirds will live in the developing world, where the number of Internet users will have doubled in five years: from 974 million in 2009 to 1.9 billion in 2014.[36] Despite this rapid growth, a significant digital divide persists: Internet penetration in developing countries is still only 32 per cent compared to a global average of 40 per cent. Globally, 4 billion people are not yet using the Internet, and more than 90 per cent of them live in the developing world.[37]

Figure 1.
Total Individuals using the Internet in Developing and Developed Countries, 2005-2014



*Estimated

Source: ITU World Telecommunication/ICT Indicators database

In terms of regions, 19 per cent of Africa's population will be online by the end of 2014, up from 10 per cent in 2010, but still trailing other regions. Europe has the highest Internet penetration worldwide, set to reach 75 per cent by the end of 2014, followed by the Americas (65 per cent), the Commonwealth of Independent States (56 per cent), the Arab States (41 per cent) and the Asia-Pacific region (32 per cent).[38]

Globally, more men than women use the Internet: 41 per cent of all men compared with 37 per cent of all women, or 483 million male Internet users compared with 475 million female users. This gender gap is most pronounced in the developing world, where 16 per cent fewer women than men use the Internet.[39] This discrepancy has important implications for human development.

The growth of Internet access is supported by increasing broadband and mobile phone penetration. The emergence of broadband has been particularly significant in facilitating online child sexual abuse and exploitation because it enables the exchange of larger files, including files containing photos, video and audio.

Globally, fixed broadband growth is slow; the growth rate was 4.4 per cent in 2014. This is mostly due to a slowdown in developing countries, where fixed broadband penetration growth rates are expected to drop from 18 per cent in 2011 to 6 per cent in 2014.[40] In contrast, mobile-broadband subscriptions (figure 2) are the fastest growing market segment. By the end of 2014 they will stand at 2.3 billion, at which time 55 per cent of all mobile-broadband subscriptions are expected to be in the developing world, compared with only

35 'Key statistical highlights: ITU data release June 2012' retrieved 25 October 2013 from <www.itu.int/ITU-D/ict/statistics/material/pdf/2011%20Statistical%20highlights_June_2012.pdf>.

36 ITU, *The World in 2014. ICT facts and figures*, International Telecommunication Union, 2014, p. 5.

37 Ibid.

38 Ibid.

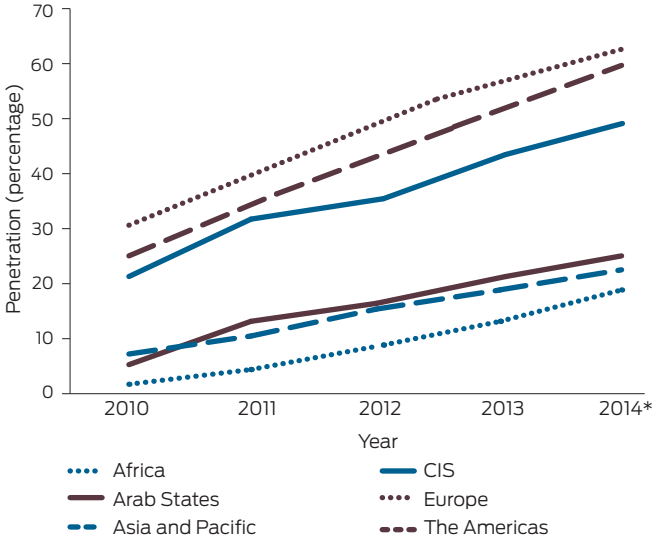
39 All figures from ITU, *The World in 2013. ICT facts and figures*, ITU, February 2013, p. 2.

40 ITU, *The World in 2014. ICT facts and figures*, International Telecommunication Union, 2014, p. 4.

20 per cent in 2008.[41] Again, Africa has the lowest level of mobile-broadband penetration (19 per cent), but the growth rate in this region is over 40 per cent—twice the global average.

By the end of 2014, the Asia-Pacific region will have almost 1 billion mobile-broadband subscriptions. Yet this region's penetration rate (23 per cent) lags behind that of other regions, including the Arab States (25 per cent) and the Commonwealth of Independent States (49 per cent).[42] It is estimated that mobile broadband subscriptions will approach 70 per cent of the world's total population by 2017.[43]

Figure 2.
Penetration of mobile-broadband subscriptions by region, 2010-2014

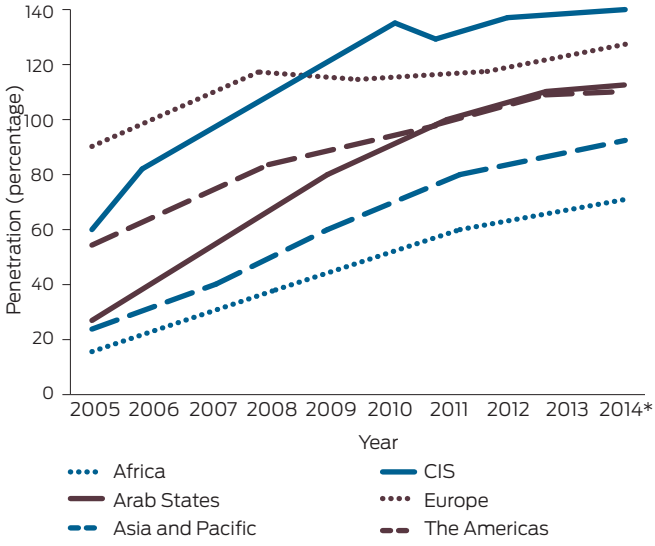


* Estimated

Source: ITU World Telecommunication/ICT Indicators database

Mobile-cellular subscriptions (figure 3) are set to reach almost 7 billion by the end of 2014. This means that there are now almost as many subscriptions as people in the world. With a global penetration rate of 96 per cent, the market is approaching saturation levels, and the current global growth rate of 2.6 per cent is the lowest ever. The strongest growth is in Africa and Asia and the Pacific, where penetration will reach 69 per cent and 89 per cent respectively by the end of 2014. Since 2012, penetration rates in countries in the Commonwealth of Independent States, the Arab States, the Americas and Europe have reached levels above 100 per cent, and are now expected to grow at less than 2 per cent in 2014.[44]

Figure 3.
Penetration of mobile-cellular subscriptions by region, 2005-2014



* Estimated

Source: ITU World Telecommunication/ICT Indicators database

2.1. Children, ICTs and the Internet

Literacy now is not just learning to read and write but learning how to use a computer.

16-year-old girl, Alexandria, Egypt[45]

The manner in which children and young people engage through ICTs is significantly different to that of previous generations. Children, for example, tend to shift easily between real and virtual worlds, and they regard the online/offline distinc-

41 Ibid., p. 2.

42 Ibid.

43 Cited in United Nations Office on Drugs and Crime, *Comprehensive Study on Cybercrime*, United Nations, 2013, p. 1.

44 ITU, *The World in 2014. ICT facts and figures*, International Telecommunication Union, 2014, p. 3.

45 Bachan, Keshet, Sarah Stevenson and Nikki van der Gaag, 'Girls in Cyberspace: Dangers and opportunities', Plan International, n.d. (circa 2010), p. 3.

tion as ever less relevant.[46] This being the case, if online opportunities are to be cultivated and online threats effectively addressed, adults must endeavour to grasp the complexities of children's online practices. The better we understand children's ICT usage patterns and online behaviour, the better we will be able to promote the immense benefits of this technology, while mitigating the risks associated with it.

A recent survey in Latin America underlines the significance of the online environment for children. It found that a third of adolescents use the Internet for two to three hours every day, and 14 per cent use it more than eight hours daily (see table 2). Similar results emerged in Europe in a survey of 25,000 Internet users aged 9 to 16 across 25 European countries, together with one parent of each child. Conducted from 2009 to 2011 by the European Union Kids Online initiative, it found that 93 per cent of children go online at least weekly, and 60 per cent go online every day.[47] In comparison, 49 per cent of European parents use the Internet daily, while 24 per cent do not use it at all. The more parents use the Internet, the more likely it is that their children will also use it often (thus gaining the skills and benefits associated with going online), and the more effectively they can mediate their children's Internet use.[48]

The online gap between children and their parents or caregivers is underlined by the disparity in the amount of time parents believe their children are spending online and the amount of time children say they spend online. A 2009 survey of 9,000 adult and child Internet users in 12 countries found that children were spending twice as much time on the Internet as their parents believed—an average of 39 hours per month.[49] Furthermore, one third of children in Europe say they sometimes ignore what their parents say about using the Internet; 7 per cent said they did this "a lot", and another 29 per cent "a little".[50]

Age has an important influence on how children operate online. Data on young children are scarce, but evidence points to a decline in the age at which children begin to interact with ICTs and use the Internet.[51] A study conducted in the United States in May-June 2013 suggests that the relative simplicity of many mobile devices is making digital entertainment and Internet content available to children under the age of 2.[52] It is reported that in wealthier East Asian countries very young children are often given touchscreen devices to keep them occupied.

Table 2.
Internet use by young people aged 13-18 in nine Latin American countries, 2013

Hours of Internet use per day	Per cent of children
1 hour or less	13
2 to 3 hours	33
4 to 5 hours	28
6 to 7 hours	12
More than 8 hours	14

Note: Survey covered 1,189 adolescents in Argentina, Chile, Colombia, Costa Rica, Mexico, Paraguay, Peru, Uruguay and Venezuela.

Source: Red Regional por el RDerecho de Niños, Niñas y Adolescentes al Uso Seguro y Responsable de las TIC (RedNATIC)

Likewise, in Europe there is an emerging trend for very young children to use Internet-connected devices, especially touchscreen tablets and smartphones.[53] The EU Kids Online initiative found that

[46] Livingstone, Sonia, Lucyna Kirwil, Cristina Ponte and Elisabeth Staksrud, with members of the EU Kids Online Network, 'In Their Own Words: What bothers children online?' LSE and EU Kids Online, 2013, p. 14.

[47] Livingstone, Sonia., Leslie Haddon, Anke Görzig and Kjartan Ólafsson, with members of the EU Kids Online Network, *EU Kids Online II, Final report*, LSE and EU Kids Online, 2011, p. 12.

[48] Ibid.

[49] Cited in UNICEF Innocenti Research Centre, *Child Safety Online: Global challenges and strategies. Technical report*, UNICEF, 2012, p. 3.

[50] Duerager, Andrea and Sonia Livingstone, 'How Can Parents Support Children's Internet Safety?', EU Kids Online, n.d., p. 4.

[51] Indeed, given the shortage of data on the youngest children, the age of online 'initiation' might be lower still.

[52] As reported in Tamar Lewin, 'New Milestone Emerges: Baby's first iPhone app', *New York Times*, 28 October 2013, p. A17.

[53] Holloway, D., L. Green and S. Livingstone, 'Zero to Eight. Young children and their internet use', LSE and EU Kids Online, 2013, p. 4.

in the five to six years preceding the start of its survey in 2009, there had been a substantial increase in Internet use by European children under 9 years of age. The rise was not consistent across countries, but rather followed usage patterns among older cohorts of children: in countries where more children use the Internet, they also tend to go online at an earlier age.[54] Video-sharing sites are popular with very young children and are one of the first sites they visit. Children under 9 years old also enjoy other online activities, including playing games, searching for information, doing homework and socializing with friends. Increasingly, research is demonstrating the importance of digital technology as a learning tool that, when used appropriately, can promote the linguistic, cognitive and social development of young children.[55]

EU Kids Online found that older children also engage in a range of diverse and potentially beneficial activities online. All European children in the age group 9 to 16 use the Internet for schoolwork and playing games alone or against the computer. In addition, 86 per cent of children watch video clips online. The majority of children (75 per cent) also use the Internet interactively for communication, including email, instant messaging and social networking (see box 2) and reading or watching the news. (These activities are pursued by two thirds of children aged 9 to 10, but only a quarter of those aged 15 to 16). Across Europe, 56 per cent of 9- to 16-year-olds play with others online, download films and music, and share content peer to peer, such as via webcam or message boards. Only 23 per cent of children advance to using the Internet for creative activities such as file-sharing, blogging, visiting chat rooms and spending time in a virtual world. Even among children aged 15 to 16, only one third do several of these activities.[56]

Like age, gender also influences how children operate online. For example, data from the EU Net Children Go Mobile, a 2013 survey of 2000 children aged 9 to 16 in seven European countries,[57] found that teenage girls tend to use the Internet to engage in communication practices and entertainment activities and are more likely to post photos, videos or music to share with others. Boys of all ages play games more.[58]

One of the most significant challenges to understanding children's use of ICTs and engagement with the Internet is the lack of research from developing countries. These countries are both home to the majority of the world's children and young people, and the places where Internet access is now growing most rapidly. This represents an important gap in our knowledge.

Steps are beginning to be taken to address this imbalance. For example, in the online survey conducted in Latin American countries referenced in table 2, 83 per cent were in either total or partial agreement with the statement that "quality access to the Internet is a fundamental right", but only 43 per cent believed this right was being realized in their own country.

Regarding online risks, 27 per cent agreed completely with the statement that "young people know the risks of cyberspace," and another 44 per cent were in partial agreement, while 29 per cent were in partial or complete disagreement with this statement. A much clearer pattern emerges for the statement that "technology is not bad, it depends on the individual and the use he or she makes of it". Two thirds (67 per cent) of adolescents agreed completely with this statement and 23 per cent agreed partially. Only 10 per cent disagreed somewhat or totally.

54 Ibid.

55 Ibid., p. 14.

56 Livingstone, Sonia, et al., *EU Kids Online II, Final Report*, op. cit. p. 14.

57 The project also included a survey of the children's parents. It was conducted in Denmark, Italy, Romania and the United Kingdom between May and July 2013.

58 Mascheroni, G. and K. Ólafsson, *Net Children Go Mobile: Risks and opportunities*, second edition, Educatt, 2014, p. 26.

Box 2.
The significance of social networking for children and young people

Social media, like Facebook and other social networks, are resources that adolescents use a lot. They are great means to communicate their rights and responsibilities to teenagers, as well as the ways and possible methods they can use to defend themselves from others. As adolescents, they can advise people, from their own point of view, about their rights and responsibilities and how they need to be dealt with.

Teenage girl, Argentina, from an interview conducted by Chicos.net, member organization of RedNATIC[59]

Social networking sites play an important role in the lives of many young people. The sites offer a range of opportunities, including the possibility of staying connected with friends; developing new social contacts with peers with similar interests; sharing self-expression content, such as art, music and political views; and developing and expressing individual identity.[60] In addition, as the quote above illustrates, they offer young people an important opportunity to learn about their rights, how to communicate them to others and how to stay safe.

In Brazil, for example, using the Internet for "visiting a social networking profile or page" is an activity pursued by 68 per cent of children aged 9 to 16, making it the second most common Internet activity after schoolwork, which draws 82 per cent of children in this age group. Overall, 70 per cent of children aged 9 to 16 who are Internet users claim to have their own profiles on social networking sites.[61] Even a significant share of younger children have a profile: 42 per cent of Brazilian children aged 9 to 10 reported having their own profile, and the number rises to as much as 71 per cent for children aged 11 and 12.[62] For most social networking sites, users aged 9 to 12 should not have accounts, according to the terms of service established by the providers of these services.

At the same time, social networking sites present a number of significant risks for children, all the more when they do not understand, or fail to apply, appropriate privacy settings. It has been found that 25 per cent of children in Brazil have the privacy setting on their social networking site set to 'public', meaning that anyone can see them.[63] In Europe younger children are more likely than older to have their profile 'public'. In fact, as a result of information and sensitization initiatives, older children seem more aware of the risks they may be exposed to by placing private information in the public domain. Furthermore, many younger and some older children do not understand the features designed to protect children from other users.[64]

Risks for children associated with online social networking include:

- Cyberbullying;
- Sharing personal information;
- Vulnerability to predatory adults;
- Sharing inappropriate or intimate photos or videos;
- Exposure to groups that share harmful or even illegal information or content;
- Exposure to large amounts of commercial advertising that, in addition, may not be age appropriate;
- Identity theft; and
- Reduced amount of time for physical activity.[65]

Generally, the risks children encounter are not exclusively associated with social networking sites, but they are often heightened by the ease of access to and use of these interactive multimedia platforms.

59 Entrevistas – RedNATIC', Canal Chicosnet, retrieved 17 July 2014 from <www.youtube.com/watch?v=VFEY-ZvbgoI>.

60 American Academy of Child and Adolescent Psychiatry, 'Children and Social Networking', *Facts for Families*, no. 100, November 2011, retrieved 6 June 2014 from <www.aacap.org/App_Themes/AACAP/docs/facts_for_families/100_children_and_social_networking.pdf>.

61 Barbosa, A., B. O'Neill, C. Ponte, J.A., Simões and T. Jereissati, 'Risks and Safety on the Internet: Comparing Brazilian and European children', LSE and EU Kids Online, 2013, p. 11.

62 Ibid., p. 12.

63 Ibid.

64 Risks and safety on the Internet, the perspective of European children—initial findings from the EU Kids Online Survey of 9 to 16 year olds and their parents, London School of Economics and Political Science, 2010, p. 43.

65 American Academy of Child and Adolescent Psychiatry, 'Children and Social Networking', *Facts for Families*, no. 100, November 2011, retrieved 6 June 2014 from <www.aacap.org/App_Themes/AACAP/docs/facts_for_families/100_children_and_social_networking.pdf>.

Furthermore, based on the findings of this survey, many adolescents in Latin America appear to demonstrate a degree of pragmatism regarding the possibility of encountering risks online. "In order to benefit from all the possibilities that technology offers", 26 per cent of adolescents in the RedNATIC survey indicated that it was necessary to take some risks; 26 per cent acknowledged that they would encounter possible dangerous sites without wishing to; and 12 per cent said that they explored sites irrespective of what they found there. Another 13 per cent indicated that they agreed with all three of the above mentioned statements, while 23 per cent of respondents disagreed with all of them.[66]

In 2013, UNICEF launched a study of the growing community of new Internet users in Kenya. Based on focus-group discussions with young people aged 12 to 17, this study looked at digital access and knowledge and emerging practices. One of the main sentiments expressed by the participants is that digital tools provide one of the few opportunities to create and explore personal identities away from the influence or interference of family members.[67] The devices most commonly used are mobile phones with Internet access or computers in an Internet café. (Mobile phone penetration is over 75 per cent across the country, and Internet penetration stood at 28 per cent in mid-2012.)[68]

This study points to a significant knowledge gap between parents and children when it comes to Internet use, especially social media. Many young people in the study reported that their parents and caregivers have a low level of digital literacy, especially among those living in poorer urban or rural neighbourhoods. Concealing or lying about their use of social networks was also commonly reported among young people. Parents, caregivers and teachers were rarely cited as sources of support in cases of online bullying or harassment.[69] Significantly, the online gap between children and parents appears to be less extreme in Europe, where levels of parental digital literacy are higher. In this region, two thirds of children say their parents know a lot (32 per cent) or quite a lot (36 per cent) about what they do online, and they are generally positive about the steps their parents take to ensure that they remain safe online (27 per cent of children indicated that they were "very positive", and 43 per cent were "a bit" positive about their parents' actions).[70]

The UNICEF study in Kenya also found that adolescents commonly befriend people online whom they have never met in person. Similarly, in a survey conducted in 2010 and 2011 of young people's interaction on MXit, the most widely used social networking platform in South Africa, 42 per cent of respondents stated that they spoke to strangers every day using the platform, and 33 per cent said that they did so at least once a week.[71] Indeed, the tendency to make little or no distinction between friendship in the online and offline environments is another characteristic that distinguishes younger Internet users from older generations. This difference is crucial in understanding young people's perceptions and online habits. The study found that adolescents:

... have a blurred distinction between online-only and other friends from their schools, neighborhoods, or other areas of their daily lives. Whether their friends are those they meet at school every day, or individuals they only know through Facebook chats, these young people refer to those in both groups as their friends.[72]

66 RedNATIC, 'Estado de situación sobre el derecho de la niñez y la adolescencia al uso seguro y responsable de las TIC en 10 países de América Latina', draft version, p. 80.

67 Pawelczyk, Kate, 'Kenya study looks at the growing community of new Internet users', retrieved 28 October 2013 from <www.unicef.org/infobycountry/kenya_70525.html>.

68 Ibid.

69 Ibid.

70 Livingstone, Sonia, et al., *EU Kids Online II, Final Report*, op. cit., p. 35.

71 Beger, Gerrit, Priscillia Kounkou Hoveyda and Akshay Sinha, 'From 'What's your ASLR' to 'Do You Wanna Go Private?'', Digital Citizenship Safety/UNICEF, 2011, p 12.

72 UNICEF, *A (Private) Public Space. Examining the use and impact of digital and social media among adolescents in Kenya*, UNICEF, 2013, p. 3.

Communication with peers is fundamentally important to many young people, and mobile phones provide them with the opportunity to remain in continuous contact, by voice, SMS and instant messaging. Mobile phone use among children has jumped in recent years, and the age at which children acquire their first mobile phone is dropping.[73]

The growing popularity of sophisticated mobile phones with Internet connectivity also means that many online activities previously undertaken via computers in fixed locations are now being conducted on smartphones. When children have access to this technology it becomes more difficult for parents or caregivers to monitor their online activity, introduce filtering or blocking mechanisms, or control their degree of Internet access.[74]

Recent European data suggest that Internet access while on the move—such as on the way to school or when out and about—is still limited although on the rise. More specifically, only 7 per cent of the 2,000 children surveyed for the Net Children Go Mobile project say they access the Internet several times a day when out and about, and 10 per cent use the Internet on the move at least daily.[75] The oldest children in this sample of 9- to 16-year-olds were far more likely to access the Internet at least daily when out and about than any other age group (33 per cent of teenagers aged 15 to 16).[76]

Social engagement is now a fundamental part of children's and young people's lives. As the functions of chat rooms, discussion forums, gaming, email, instant messaging and social networking begin to merge, the boundaries between them are ceasing to have validity for children.[77] In turn, this contributes to the deconstruction of traditional boundaries of privacy by creating situations in which children engage in 'chat' or conversation in apparently private settings while in fact exposing themselves, wittingly or unwittingly, to an unknown, worldwide audience. To take just one example, a study from 2011 of children and young people's use of digital technology in Ukraine found that 46 per cent of Internet users aged 10 to 17 gave out their personal mobile phone number on a social networking site while 36 per cent shared their home address and 51 per cent shared personal photos.[78]

The inclination to share personal details is compounded by a tendency among young people to act impulsively and a common expectation that online environments can and will provide them with immediate gratification. This immediacy means that children and young people may not take into account the consequences of their online actions or may fail to identify online dangers. Moreover, the warning signs that can serve to protect children in the physical world—including physical and behavioural cues, and the appraisal of friends or caregivers—are largely absent online.[79]

[73] UNICEF, 'Child Safety Online. Global challenges and strategies. Technical report', 2012, p. 22.

[74] Ibid., p. 23.

[75] Mascheroni, G. and K. Ólafsson, *Net Children Go Mobile: Risks and opportunities*, second edition, Educatt, 2014, p. 12.

[76] Ibid.

[77] UNICEF, *Child Safety Online. Global challenges and strategies. Technical report*, 2012, p. 22.

[78] Microsoft and UNESCO, 'Рівень обізнаності українців щодо питань безпеки дітей в Інтернеті' [The level of awareness of the Ukrainians on the safety of children using the Internet] 2011, cited in Gerrit Beger, Priscillia Kounkou Hoveyda and Akshay Sinha, 'The UaNet Generation. An exploratory study of the Ukrainian digital landscape', Digital Citizenship Safety/UNICEF, 2011, p. 16.

[79] UNICEF, 'Child Safety Online. Global challenges and strategies. Technical report', 2012, p. 24.

© UNICEF/INDA2011-00389/Vishwanathan

3. International standards

3.1. The Convention on the Rights of the Child and its Optional Protocols

The Convention on the Rights of the Child (CRC) does not specifically refer to online protection of children's rights. Indeed, 1989, the year the United Nations General Assembly adopted the CRC, was the same year that Tim Berners-Lee of the European Laboratory for Particle Physics developed the World Wide Web, a new technique for distributing information on the Internet. The term 'Internet' had been used for the first time only seven years earlier.

Nonetheless, the CRC and its Optional Protocols, notably the Protocol on the sale of children, child prostitution and child pornography (OPSC), provide important guidance for realization of children's rights online. They call for all measures, including legislative, policy and educational initiatives, to be guided by the best interests of the child; to respect and support children's growing autonomy and agency; and to protect children from violence and discrimination. These general principles help to capitalize on the potential of the online environment to promote children's learning and freedom of expression; to support children in accessing, receiving and imparting information; and to protect them from harmful materials and information, from unlawful interference with their privacy or correspondence, and from situations where their honour and reputation may be at risk.

Similarly, these general principles help to realize the potential of ICTs to provide children with information on the promotion of their rights, and to seek support and redress when they are exposed to violence, abuse and exploitation.

Guided by these standards, it is crucial to ensure that all children, including the most marginalized, enjoy the same degree of access to the Internet and benefit from the protection they all require. This is particularly important given the digital divide that has opened up among children, between those who have ready and convenient access to the Internet at home, school and elsewhere, and those who do not; between those who regularly benefit from guidance and advice from their parents or schools, and those who explore the cyber space on their own and lack any support; and between those who are confident and proficient users of the Internet and those who are not.

Child victims of violence, whether online or offline, come from all walks of life. But factors such as age, disability or social exclusion can have an important bearing on children's online activities and on children's ability to cope with potential risks.

Younger children may lack the capacity to identify risks. Other vulnerable children—including those out of school, from poor backgrounds or a minority community, and children with disabilities—may be less likely to enjoy the benefits offered by the online environment or to receive information regarding safe Internet use. They may also be more likely to be bullied, harassed or exploited online. Without decisive action, the digital divide threatens to reinforce or exacerbate existing patterns of disadvantage.

In the case of Internet use, opportunities and risks are inextricably linked, and it is crucial to balance the rights enshrined in the CRC that facilitate a child's participation in the online environment and those intended to ensure a child's safety and protection. This becomes particularly clear when considering, for example, the use of filtering and blocking tools to prevent children's access to online content or information considered harmful or inappropriate for their age.

Also in such cases it is crucial to ensure that the best interests of the child are a primary consideration at all times and that the evolving capacities of children and young people are given due attention. In other words, the relative degree of freedom or protection a child should receive online depends upon his or her level of development and capacity to cope with risks. Furthermore, while all children must enjoy freedom of expression, this should not be construed as a justification for causing hurt or harm or damaging the rights or reputations of oth-

ers. This is an important consideration in terms of peer-to-peer cyberbullying or cyber harassment.

The CRC does not specifically criminalize child sexual abuse images, although a prohibition on this material is implicit in, for example, the child's right to protection against "arbitrary or unlawful interference with his or her privacy" and to "unlawful attacks on his or her honour and reputation" under article 16. The OPSC, to which 167 States are parties at the time of writing, also provides important guidance in this respect (see box 3).

In recent years, the Committee on the Rights of the Child has given increasing attention to ICTs and the Internet in its concluding observations to periodic reports on the CRC and OPSC. Its recommendations have highlighted crucial areas requiring further efforts, including the adoption of "a national coordinating framework to address all forms of violence against children, including on the Internet";[80] passage of comprehensive legislation "to criminalize all forms of child pornography and sexual exploitation of children on the

Box 3.
The Optional Protocol to the CRC on the sale of children, child prostitution and child pornography

Article 1 of the OPSC requires States parties to "prohibit the sale of children, child prostitution and child pornography",[81] where child pornography is, "[...] 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."[82]

Article 3 requires that each State party ensure that, as a minimum, "[p]roducing, distributing, disseminating, importing, exporting, offering, selling or possessing [...] child pornography" is "fully covered under its criminal or penal law, whether such offences are committed domestically or transnationally or on an individual or organized basis".[83]

The OPSC requires that countries criminalize possession with the intent to distribute, disseminate, sell.[84]

The OPSC also gives consideration to the obligations of States Parties to fight impunity. Article 4 requires each State party to "take such measures as may be necessary to establish its jurisdiction over the offences [...], when the offences are committed in its territory or on board a ship or aircraft registered in that State."

Given the global nature of the Internet and the international dimension that characterizes much online violence, exploitation and abuse, article 6 calls on States parties to "afford one another the greatest measure of assistance in connection with investigations or criminal or extradition proceedings [...] including assistance in obtaining evidence at their disposal necessary for the proceedings."[85]

Under article 9, States parties are required to "adopt or strengthen, implement and disseminate laws, administrative measures, social policies and programmes" to prevent the offences it refers to. Paying special attention to especially vulnerable children is another concern expressed,[86] as well as "awareness in the public at large, including children, through information by all appropriate means, education and training, about the preventive measures and harmful effects of the offences referred to in the present Protocol."[87] Article 9 also addresses the important issue of rehabilitation and compensation for children who have fallen victim to offences involving images of child sexual abuse.

80 Concluding observations on the combined third and fourth periodic reports of Luxembourg, adopted by the Committee at its sixty-fourth session (16 September–4 October 2013), 29 October 2013. CRC/C/LUX/CO/3-4, §30(b).

81 Optional Protocol to the CRC on the sale of children, child prostitution and child pornography, article 1.

82 Ibid., article 2(c).

83 Ibid., article 3(1).

84 Optional Protocol to the CRC on the sale of children, child prostitution and child pornography, article 6(1).

85 Ibid., article 9(1).

86 Ibid., article 9(2).

87 See ECPAT, 'Protection and the OPSC: Justifying good practice laws to protect children from sexual exploitation', ECPAT International, Journal series no. 2, 2012, p. 16.

Internet"[88] and the "solicitation of children for sexual purposes and accessing child pornography by means of information and communication technology"; [89] and measures to prevent publication and dissemination of pornographic material concerning children through surveillance mechanisms to automatically block offending Internet service providers (ISPs) and other media, and taking prompt steps to establish an authority for Internet safety, ISP licensing and checks for content harmful to children.[90]

The Committee's Day of General Discussion on 'Digital media and child rights', held in September 2014, contributed to further broadening the scope of the Committee's reflections in this area and to the development of rights-based strategies to maximize online opportunities for children while protecting them from risks and possible harm.

3.2. Other international standards to safeguard children's online protection

In recent years significant standards have been adopted to combat cybercrime and protect children from risks online. These include the UN Convention against Transnational Organized Crime, international labour standards and important regional legal instruments. International Labour Organization Convention 182 on the Worst Forms of Child Labour recognizes in article 3 "the use, procuring or offering of a child for prostitution, for the production of pornography or for pornographic performances" among "the worst forms of child labour" that need to be prohibited and eliminated.

The Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse is the first treaty to address children's protection from sexual violence in the face of challenges presented by technological developments, and to identify as an offence the solicitation of children for sexual purposes through ICTs, often known as 'grooming'. The Council of Europe Convention on Cybercrime criminalizes offences against and through computer systems, including child pornography; provides law enforcement with effective means to investigate cybercrime and secure electronic evidence; and offers a framework for international police and judicial cooperation in computer related cases involving crimes against children. Both conventions can be adhered to by States from other regions.

Combating cybercrime is also addressed by the 2001 Agreement on Cooperation in Combating Offences related to Computer Information, developed by the Commonwealth of Independent States, and the 2010 Arab Convention on Combating Information Technology Offences, promoted by the League of Arab States. The African Union's draft Convention on the Establishment of a Legal Framework Conducive to Cybersecurity in Africa anticipates the criminalization of cybercrime activities, including computer-related harassment, extortion or causing personal harm, and the production, distribution or possession of child pornography.

---

88 Concluding observations on the combined third and fourth periodic reports of China, adopted by the Committee at its sixty-fourth session (16 September–4 October 2013), 29 October 2013. CRC/C/CHN/CO/3-4, §45(d).

89 Concluding observations on the report submitted by Portugal under article 12, paragraph 1, of the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography, 31 January 2014. CRC/C/OPSC/PRT/CO/1, §26(a).

90 Concluding observations on the second periodic report of the United States submitted under article 12 of the Optional Protocol to the Convention on the sale of children, child prostitution and child pornography, adopted by the Committee at its sixty-second session (14 January–1 February 2013), 2 July 2013. CRC/C/OPSC/USA/CO/2, & 28(a&b).

4. Understanding online risks and harm

A degree of risk is inherent in the use of the Internet and ICTs, but this risk does not inevitably translate to harm for children and young people. In other words, a child may take or encounter risks online without experiencing abuse or harm.[91] The EU Kids Online final report sets out some of the key risks associated with children's online activity (see table 3).[92]

It is important to recognize that teaching digital skills to children does not generally reduce online risks. On the contrary, more skills present children with more online opportunities, and opportunities are, in turn, associated with risk. One reason for this is that children must explore and encounter some risks in order to learn and gain resilience (see box 4). However, more skills can also reduce the harm that children experience as a result of encountering online risk.[93]

The more children in a country who use the Internet daily or frequently, the greater the likelihood that they have encountered or will encounter online risks. Frequent use is, at the same time, also likely to bring more opportunities.[94] In every situation, even where children have an active role in creating risk, it is crucial that they be acknowledged as victims.[95]

The EU Kids Online report noted that only 12 per cent of children aged 9 to 16 who use the Internet say they have been bothered or upset by something online. Most children did not report being bothered or upset by going online, and most risks were encountered by less than a quarter of children.[96] This is not to diminish the impact of harm when it occurs: as many as 80 per cent of adolescents in the RedNATIC survey of nine Latin American countries agreed fully or partially with the affirmation that, "there are behaviours on the Internet that cause more harm/injury than blows".[97]

Table 3.
Online risks: children as recipients, participants and actors

	Child as recipient (online content)	Child as participant (online contact)	Child as actor (online conduct)
Commercial	Advertising, spam, sponsorship	Tracking or harvesting personal information	Gambling, illegal downloads, hacking
Aggressive	Violent, gruesome, hateful content	Being bullied, harassed or stalked	Bullying or harassing another
Sexual	Pornographic or harmful sexual content	Meeting strangers, being groomed	Creating/uploading pornographic material
Values	Racist or biased information or advice	Self-harm, unwelcome persuasion	Providing advice e.g., suicide, pro-anorexia

[91] UNICEF, 'Child Safety Online. Global challenges and strategies. Technical report', 2012, p. 26.

[92] Livingstone, S. and L. Haddon, *EU Kids Online*, LSE and EU Kids Online, 2009, p. 10.

[93] Livingstone, Sonia, et al., *EU Kids Online II, Final Report*, op. cit., p. 42.

[94] Ibid., p. 11.

[95] UNICEF, *Child Safety Online. Global challenges and strategies*, UNICEF, 2011, p. 17.

[96] Livingstone, S., L. Haddon, A. Görzig and K. Ólafsson, 'Risks and Safety on the internet: The perspective of European children. Initial findings', LSE and EU Kids Online, 2010, p. 11.

[97] RedNATIC, 'Estado de situaciòn sobre el derecho de la niñez y la adolescencia al uso seguro y responsible de las TIC en 10 países de América Latina', draft version, p. 105.

Box 4.
Strategies to enhance children's resilience online[97]

Open communication with children, both at home and at school, about issues concerning the online environment;

Opportunities for children to learn how to use online coping strategies—such as deleting messages, blocking contacts and reporting providers of inappropriate content—from an early age;

Appropriate support for children to tackle their psychological problems and build self-confidence, with special attention for vulnerable children;

Parental Internet access and use, which both cultivates the confidence of parents and caregivers and enhances their ability to provide guidance to children;

Positive attitudes about online safety and proactive coping strategies among peer groups;

Support for children's Internet use and safety by schools and teachers, both technical support and assistance in developing problem-solving strategies;

Action by parents to address online risk, including monitoring and mediation rather than simply restricting children's Internet use.

Source: EU Kids Online

The UNICEF study of adolescents in Kenya found very low awareness of the risks and consequences of engaging in unsafe behaviour online. It also found that young people have only an abstract sense of the risks associated with their use of digital and social media, and many believe that the repercussions of risky behaviour only happen to other people.[98]

Some of these young people do not believe there is risk involved in meeting 'friends' with whom they have only interacted online or engaging in suggestive self-exposure.[99]

A particularly troubling finding with respect to children's exposure to risk and harm on the Internet is the extent to which parents are unaware of their child's experience or underestimate their exposure (see table 4).

Table 4.
Parents' incorrect beliefs about their children's online experience

Online experience of child	Per cent of parents who stated their child had not had this experience
Has seen sexual images	41
Has received sexual messages	52
Has received nasty or hurtful messages	56
Has met offline with an online contact	62

Source: EU Kids Online study[100]

Older children may themselves be complicit in creating this information gap. In a 2011 survey by GFI Software, based on interviews with 500 parents and their teenage children in the United States, 42 per cent of teens admitted they had cleared their browsing history after using the Internet in a conscious move to avoid being monitored by their parents.[101]

In considering the risks and potential harm associated with the use of ICTs, it is important to recognize that violence, exploitation and abuse are not exclusively concerns for children who are

[98] d'Haenens, Leen, Sofie Vandoninck and Verónica Donoso, 'How to cope and build online resilience', EU Kids Online, January 2013, p. 8, retrieved 26 June 2014 from <http://eprints.lse.ac.uk/48115/>.

[99] UNICEF, 'A (Private) Public Space. Examining the use and impact of digital and social media among adolescents in Kenya', UNICEF, 2013, p. 3.

[100] Livingstone, S., L. Haddon, A. Görzig and K. Ólafsson, 'Risks and Safety on the Internet: The perspective of European children. Initial findings', LSE and EU Kids Online, 2010, p. 11.

[101] GFI Software, '2011 Parent-Teen Internet Safety Report', GFI Software, 2011, p. 7.

'connected'. In other words, children—vulnerable children in particular—who have little or no contact with technology in their daily lives can still become victims of online harm. This is often the case, for example, with live streaming of sexual abuse (discussed below) or use of ICTs by sex tourists to contact intermediaries prior to making a trip to procure child victims from poor communities. Images of the abuse that subsequently ensues often end up traded on the Internet.

As noted, situations of online risk do not always result in harm, but when harm arises the impact on a child can be devastating. The use of ICTs in the commission of offences can increase levels of harm to child victims, in particular by facilitating the layering and intertwining of offences such that multiple forms of abuse and exploitation can take place simultaneously or be committed against the same victim over time. This was found in a study by the United Nations Office on Drugs and Crime (UNODC) on the effects of new information technologies on the abuse and exploitation of children. This is particularly true in cases where contact sexual abuse or exploitation is combined with an online component, for instance, the production of child sexual abuse material and its subsequent distribution online, or the trafficking of children with a view to their online exploitation.[102]

Regarding the impact of harmful content online, some children may demonstrate signs of stress from exposure to this kind of material, while others may not show any visible effects. In every case, however, exposure to explicit or harmful content has the potential to influence the child's development of values and perceptions.[103] Little is known about the coping mechanisms of child victims of online sexual abuse. Experience from the Online Project in Sweden, established by BOP-Elefanten in 2006, suggests that most often the victims of online sexual abuse exhibit symptoms similar to those of child victims of offline abuse, including eating disorders, exhaustion, pseudo-maturity, aggression, depression, post-traumatic symptom disorders, low self-esteem, shame, guilt and anxiety.[104] Sexual abuse during childhood is also known to create long-term problems for those who have been victimized. Many exhibit serious mental health issues as well as behavioural disorders and addictions.[105] The impact of sexual abuse online often extends beyond the child victim to his or her parents, caregivers and broader family members.

The perpetrators of violence, abuse or exploitation in the online environment tend to constitute a very diverse group. Some offenders operate individually, while others operate in groups or through organized criminal networks. Indeed, ICTs have facilitated the formation of groups of abusers: UNODC points to the fact that these technologies provide unprecedented access to social affirmation for offenders, through interactive online communities that form around all areas of abuse and exploitation, particularly with respect to child sexual abuse material and activities associated with grooming.[106] In terms of individual offenders, men dominate in certain categories of offences, including child sexual abuse material offences, grooming and cyberstalking. However there is a high

[102] UN Commission on Crime Prevention and Criminal Justice, 'Study facilitating the identification, description and evaluation of the effects of new information technologies on the abuse and exploitation of children', 7 May 2014, E/CN.15/2014/CRP.1, p. 15.

[103] Ibid., p. 14.

[104] Jonsson, Linda, 'Child abuse images and sexual exploitation of children online', ECPAT International, *Research Findings on Child Abuse Images and Sexual Exploitation of Children Online*, September 2009, pp. 18-19.

[105] Choo, Kim-Kwang Raymond, 'Online Child Grooming: A literature review on the misuse of social networking sites for grooming children for sexual offences', Australian Institute of Criminology, AIC Reports, Research and Public Policy Series, no. 103, 2009, p. xii.

[106] UN Commission on Crime Prevention and Criminal Justice, 'Prevention, protection and international cooperation against the use of new information technologies to abuse and/or exploit children. Report of the Secretary-General', E/CN.15/2014/7, 5 March 2014, §33. UNODC uses the term 'cyberenticement' to refer to "persuading, soliciting, coaxing, enticing, or luring by words, actions or through communication on the Internet or any electronic communication, of a minor for the purpose of engaging in sexual conduct." UNODC defines grooming as "a series of acts that facilitate cyberenticement such as actions deliberately undertaken with the aim of befriending and establishing an emotional connection with a child, in order to overcome the child's resistance in preparation for sexual activity with the child." Ibid, §12.

prevalence of women offenders for certain forms of violence and exploitation, including cyberbullying and trafficking.[107]

The remainder of this chapter examines in more detail the risks children and adolescents commonly encounter when using ICTs or going online.

4.1. Violent content

[...] *it doesn't matter whether animals or children are bullied/tortured, both are disgusting.*

11 year-old boy from Estonia[108]

As a direct result of its openness, the Internet harbours a vast range of material that, while not necessarily illegal, is potentially harmful to children and young people. A study from France indicates that 68 per cent of children aged 15 to 17, 62 per cent aged 13 to 15 and 43 per cent aged 11 to 13 have already come across "shocking" material on the Internet.[109] A comparative analysis of the situation in Brazil and Europe conducted by EU Kids Online found that content-related risks rank as the highest concern, being reported by about half of all children (58 per cent in Europe and 49 per cent in Brazil).[110]

Children and young people encounter—and may seek out—pornographic material online, and some children and young people may share this material with online and offline friends. Many young participants in the UNICEF study of digital and social media use among adolescents in Kenya reported having encountered sexually explicit content via the Internet on computers and mobile phones. Some acknowledged having shared it on DVDs and hard drives; boys well-versed in digital technologies and social media platforms were found to download and share this content more regularly.[111] In Europe, findings from EU Kids Online suggest that children commonly encounter sexual risks—seeing sexual images or receiving sexual messages online—but few of the children who are exposed to them experience them as harmful.[112]

Violent material tends to receive less public attention than sexually explicit material, but many children are particularly concerned about violent, aggressive or gory online content, including images and descriptions associated with war and other atrocities, domestic abuse and violence, and cruelty to animals. A 2013 study of 25,000 children aged 16 and under conducted for the United Kingdom Council for Child Internet Safety, the biggest study of its kind in the United Kingdom, found that children are as upset by violent videos on YouTube that feature animal cruelty or beheadings and by insensitive Facebook messages from divorced parents as they are by online bullying and pornography.[113] At the time of writing, a single, easily accessible website, which requires no minimum age for its visitors, offers an extensive gallery of harrowing and degrading images including photographs of human decomposition, dismemberment, amputation, exhumation, suicide and torture, among others. Children also report that video-sharing websites are often associated with violent and pornographic content, along with a range of other content-related risks.[114]

---

107 Ibid., §41.

108 Livingstone, Sonia, Lucyna Kirwil, Cristina Ponte and Elisabeth Staksrud, with the EU Kids Online Network, 'In their Own Words: What bothers children online?' LSE and EU Kids Online, 2013, p. 8.

109 Poll conducted by Génération numérique and cited in Dominique Baudis and Marie Derain, *Enfants et écrans : grandir dans le monde numérique*, République Française, Le Défenseur des Droits, 2012, p. 22.

110 Barbosa, A., B. O'Neill, C. Ponte, J.A., Simões and T. Jereissati, 'Risks and Safety on the Internet: Comparing Brazilian and European children', LSE and EU Kids Online, 2013, p. 16.

111 UNICEF, *A (Private) Public Space. Examining the use and impact of digital and social media among adolescents in Kenya*, UNICEF, 2013, p. 3.

112 Livingstone, S., L. Haddon, A. Görzig, and K. Ólafsson, 'Risks and Safety on the Internet: The perspective of European children. Initial findings', LSE and EU Kids Online, 2010, p. 11.

113 Brown, Maggie, 'Children are 'upset' by online violence, study finds', *The Observer*, 2 February 2013, retrieved 14 July 2014 from <www.theguardian.com/technology/2013/feb/03/children-upset-online-violence-study>.

114 Livingstone, Sonia, Lucyna Kirwil, Cristina Ponte and Elisabeth Staksrud, with the EU Kids Online Network, 'In their Own Words: What bothers children online?' LSE and EU Kids Online, 2013, p. 1.

4.2. Hateful, damaging or otherwise harmful material

The things that bother people about my age are the influence of bad websites such as how to diet or lose weight so you could be known as the pretty one.

15 year-old girl from Ireland[115]

There is a large amount of easily accessible material on the Internet that addresses—and either tacitly or explicitly encourages—harmful behaviour or ideas among children and adolescents. This includes extremist material that promotes, for example, racial and religious hatred, homophobia or misogyny. Depending on their age and evolving capacities, children may not be able to critically assess such material, or may even be drawn to it out of curiosity. A report from the Australian Human Rights Commission suggests that the nature of the Internet makes it a particularly valuable tool for racist groups because such groups do not usually have access to the regular mass media, and Internet technology is relatively simple and available at low cost. Furthermore, racist groups are often internationally organized, and the Internet facilitates international communication. Racist content on the Internet includes websites, computer games, emails, social media pages, chat-rooms, discussion groups and music merchandising.[116]

Children likewise risk exposure to websites and blogs that discuss suicide (including the efficacy of different methods of suicide), eating disorders such as anorexia and bulimia, self-harm and drug use.

The majority of these websites contain legal material, and many forums and online communities dedicated to anorexia or bulimia explicitly state that their intention is to offer support and recovery for victims of these conditions, not to encourage eating disorders. Sites related to suicide, self-harm and drug-taking often contain similar disclaimers. In practice, however, eating disorder forums frequently contain easily accessible advice from community members on how to binge and purge (and how to hide these practices from others), mutual encouragement and support in favour of extreme weight loss, disturbing messages and descriptions, and galleries of 'selfies' and aspirational 'ideal' bodies. Many community members promote the idea that eating disorders are a lifestyle choice rather than a medical condition. In some cases, blogs or websites associated with eating disorders are supported by advertisements supporting weight loss.

Children and young people's exposure to online images that reinforce gender stereotypes and thus influence gender relations represents additional grounds for concern. Likewise, material promoting the sexualization of children contributes to harmful attitudes toward children and distorts their own self-perception.

4.3. Child sexual abuse images

ICTs have significantly simplified and facilitated the production, distribution and possession of child sexual abuse images and other material. The volume of such images, both still and moving, available on the Internet is not known, although it is feasible that there are millions of such images, depicting tens of thousands of images of individual children produced to meet the demand of this market.

UNODC cites an estimated 1,500 per cent increase in the number of child sexual abuse images on the Internet from 1997 to 2006.[117] It indicates that every commercial child pornography website "is a gateway to hundreds or thousands of individual images or videos of child sexual abuse. They are often supported by layers of payment mechanisms, content stores, membership systems and advertising."[118] Recent developments in this area

115 Cited in ibid., p. 4.

116 Race Discrimination Unit, Australian Human Rights Commission, 'Examples of racist material on the Internet', retrieved 14 July 2014 from <www.humanrights.gov.au/publications/examples-racist-material-internet>.

117 UN Commission on Crime Prevention and Criminal Justice, 'Study facilitating the identification, description and evaluation of the effects of new information technologies on the abuse and exploitation of children', 7 May 2014, E/CN.15/2014/CRP.1, p. 17.

118 United Nations Office on Drugs and Crime, *Comprehensive Study on Cybercrime*, United Nations, 2013, p. 36.

include the use of sites that, when loaded directly, display legal content, but when loaded via a particular referrer gateway site enable access to child pornography images.[119]

Only a few years ago, most websites hosting child sexual abuse images were commercial, but today images of child sexual abuse are increasingly being traded on the Internet using applications such as non-commercial P2P networks.[120] Law enforcement operations against P2P file-sharing of child sexual abuse images have identified millions of Internet Protocol addresses offering child pornography.[121]

In the United Kingdom, a report by the Child Exploitation and Online Protection Centre (CEOP) noted that "[n]o evidence was found to suggest that a substantial commercial market [for indecent images of children] exists in 2012."[122] At the same time, CEOP reports that P2P decentralized networks continue to be a popular means by which offenders download and distribute child sexual abuse images, and the use of the 'Deep Web' to disseminate and access abusive images is also a growing concern.[123]

A significant proportion of child sexual abuse images online are of young children, and there is an identifiable trend of declining age of the children depicted.[124] UNODC data indicate that between 2011 and 2012 there was a 70 per cent increase in child sexual abuse material focused on girls under age 10, and abuse material involving toddlers or babies is not uncommon. These images are associated with increasing levels of violence, and a significant number of online forums and channels openly advertise videos of brutal sexual assault.[125]

Child sexual abuse images are, in turn, inextricably linked to other forms of sexual violence. This phenomenon cannot be tackled if the focus rests solely on the child sexual abuse material and does not extend to the underlying sexual violence.[126]

Equally, it is clear that sustainable and effective responses to child sexual abuse material must address and seek to minimize the enormous global demand for such images. In 2013, for example, Operation Spade, an international investigation led by the Toronto (Canada) police, led to the arrest of 348 people (108 in Canada, 76 in the United States and 164 elsewhere) tied to a massive child pornography ring. Police seized over 45 terabytes of data from the computer of the man at the centre of this ring and found 200,000 images and 400 videos. A retired teacher arrested in the operation was found to possess over 350,000 images and 9,000 videos depicting child sexual abuse.[127]

Once online, child sexual abuse images can, and do, circulate indefinitely, perpetuating the abuse. In addition to the serious harm caused to the victims of child sexual abuse images, the circulation of such images contributes to harmful social attitudes that tolerate demand for sexual activity with children.[128] The continued presence of child sexual abuse images encourages further exploitation of children, increases the number of abusers

119 Ibid.

120 UN Commission on Crime Prevention and Criminal Justice, 31 January 2011, E/CN.15/2022/2, §15.

121 US Department of Justice, 'The National Strategy for Child Exploitation Prevention and Interdiction', cited in United Nations Office on Drugs and Crime, *Comprehensive Study on Cybercrime*, United Nations, 2013, p. 36, retrieved 8 April 2014 from <www.justice.gov/psc/docs/natstrategyreport.pdf>.

122 Child Exploitation and Online Protection Centre, *Threat Assessment of Child Sexual Exploitation and Abuse*, CEOP, June 2013, p. 8.

123 Ibid.

124 UNICEF, 'Child Safety Online. Global challenges and strategies. Technical report', 2012, p. 14.

125 UN Commission on Crime Prevention and Criminal Justice, 'Prevention, protection and international cooperation against the use of new information technologies to abuse and/or exploit children. Report of the Secretary-General', E/CN.15/2014/7, 5 March 2014, §30.

126 National Rapporteur on Trafficking in Human Beings, *Child Pornography—First report of the Dutch National Rapporteur*, BNRM, 2011, p. 24.

127 See, for example, 'Hundreds held over Canada child porn', *BBC News*, retrieved 23 June 2014 from <www.bbc.com/news/world-us-canada-24944358>.

128 ECPAT, 'Protection and the OPSC: Justifying good practice laws to protect children from sexual exploitation', Journal series no. 2, ECPAT International, 2012, p. 14.

and results in children being exposed to repeated abuse that continues indefinitely.[129]

4.4. Inappropriate contact, online grooming, exploitation and trafficking

Perhaps when people hear about cybersex they think it doesn't have any physical effect, [...]. *But it can do things to your core. It can take things from you, your dignity and your purity.*

Girl from the Philippines,
forced to perform sexual acts
on webcam at 15 years of age[130]

The apparent anonymity of much online interaction, combined with the lack of social cues that condition face-to-face interaction, facilitate inappropriate advances towards children and young people online.

Results of a survey of over 42,000 women across the European Union published in 2014 by the Agency for Fundamental Rights found that 11 per cent of women had experienced inappropriate advances on social websites or been subjected to sexually explicit emails or SMS messages. This figure was higher still for young women: 20 per cent of women aged 18 to 29 had been victims of such cyber harassment.[131] When this behaviour is repeatedly carried out by the same person, it can be understood as a form of cyberstalking. Indeed, the survey found that cyberstalking concerns young women in particular, reflecting young people's greater use of and exposure to the Internet and social media.[132]

The premeditated behaviour associated with grooming is characterized by a clear power imbalance between the adult and the victim or victims.[133]

UNICEF acknowledges, however, that the publicity about online predators attempting to lure children into sexual relations through lies about their age and gender misrepresents the overall picture of online predatory behaviour. Evidence indicates that Internet sex crimes involving adults and children are more likely to fit a model of statutory rape, involving adult offenders who meet, develop relationships with and openly seduce underage teenagers, rather than a process of forced sexual assault, age deception or paedophilic child abuse.[134] A report based on research conducted in the United States suggests that most online offenders are, in fact, open about being older adults.[135] This openness potentially complicates initiatives to protect adolescents from this kind of contact risk, since these young people may not necessarily regard themselves as victims.

In certain circumstances, children might also actively seek online attention from older men in exchange for gifts or money.

Sexual abuse and exploitation in the converged online/offline environment is also associated with trafficking and sex tourism.[136] In the case of trafficking, perpetrators use ICTs to engage in real-time communication with the victim, such as through voice messages or texting. There are also many documented cases of human traffickers using social networking sites and micro-blogging services to facilitate their activities. Moreover, ICTs and the Internet allow sex buyers to search and make arrangements for sex acts with children from al-

129 UNICEF, *Child Safety Online. Global challenges and strategies*, UNICEF, 2011, pp 17.

130 Cited in Crawford, Angus, 'UK paedophiles pay to watch webcam child sex abuse in Philippines', *BBC News UK*, 15 January 2014, retrieved 12 March 2014 from <www.bbc.com/news/uk-25729140>.

131 European Union Agency for Fundamental Rights, 'Violence against Women: Every day and everywhere', Fundamental Rights Agency press release, Vienna/Brussels, 5 March 2014, p. 2.

132 European Union Agency for Fundamental Human Rights, *Violence against Women: An EU-wide survey. Main results*, Publications Office of the European Union, 2014, p. 93.

133 UNICEF, 'Child Safety Online. Global challenges and strategies. Technical report', UNICEF, 2012, p. 49.

134 Ibid., p. 40.

135 Wolak, Janis, 'Research Findings in the United States about Sexual Exploitation via Virtual Interactions' *Research Findings on Child Abuse Images and Sexual Exploitation of Children Online*, ECPAT International, September 2009, p. 7.

136 Commission on Crime Prevention and Criminal Justice, E/CN.15/2022/2, 31 January 2011, ¶16.

most anywhere.[137] Indeed, in today's connected world, the use of mobile technology or some form of emailing or messaging in trafficking operations is becoming increasingly common. In June 2014, authorities in the United States rescued 168 children and arrested 281 alleged pimps in more than 100 cities across the country. The Federal Bureau of Investigation reported that a number of these children had been sold online.[138]

Sex tourism is also increasingly facilitated by ICTs and the Internet. For example, sexual abusers of children research national situations online, consult members of their clandestine communities prior to travelling and contact national operators who can furnish them with child victims. Victims of child sex tourism often come from socioeconomically disadvantaged backgrounds or are members of ethnic minorities, displaced communities and other marginalized social groups.[139]

Likewise, poverty and marginalization are often associated with the emerging phenomenon of child sexual abuse live streaming, whereby offenders target vulnerable families overseas to facilitate live access to children over webcam. The children are made to engage in sexual activity in exchange for payment to the family or an organized crime group.[140] Terre des Hommes refers to this phenomenon as webcam child sex tourism, defining it as adults offering "payment or other rewards to direct and view live streaming video footage of children in another country performing sexual acts in front of a webcam."[141] Based on its work in the Philippines, Terre des Hommes indicates that most victims are girls from economically disadvantaged backgrounds. Children involved in this form of sexual exploitation generally perform webcam sex shows from their home computers, Internet cafes or 'dens'—buildings in which several women and children are employed or kept against their will.[142] As broadband access becomes cheaper and more widely available, incidents such as these are likely to increase.

4.5. Cyberbullying

I am a member of "SchülerVZ" [German online community for students]. *And once I was badly insulted because of my physical disability. That was totally uncool and I felt really bad.*

16-year-old boy, Germany[143]

Cyberbullying may include spreading rumours; posting false information or nasty messages, embarrassing comments or photos; or excluding someone from online networks or other communications. Characterized by an imbalance of power, the harm it causes can be profound. This is partly because the Internet permits this behaviour to intrude into a child's private space, offering no room for escape, and partly because the online reach of hurtful messages or images is so much greater than for offline bullying.

As noted by UNODC, those involved in cyberbullying use websites and social media to expand their audience and increase the impact of their actions on the victim: "Use of such platforms enables perpetrators to quickly and easily enlist others to gang up on the victim. The semi-anonymous nature of the Internet may increase the viciousness of perpetrators and aggravate the harm of the initial bullying."[144]

137 Hughes, Donna M., 'Prevention of trafficking on human beings online', keynote address, *Seventh EU Anti-Trafficking Day. Links between the Internet and Trafficking in Human Beings*, 18 October 2013, Vilnius, Lithuania, p. 4.

138 'FBI recovers 168 children in child sex trafficking sting', *BBC News*, 23 June 2014, retrieved 24 June 2014 from <www.bbc.com/news/world-us-canada-27989447>.

139 ECPAT International, 'End child sex tourism', retrieved 24 June 2014 from <www.ecpat.net/end-child-sex-tourism>.

140 Child Exploitation and Online Protection Centre, 'Threat Assessment of Child Sexual Exploitation and Abuse', CEOP, June 2013, p. 8.

141 Terre des Hommes, 'Webcam Child Sex Tourism. Becoming Sweetie: A novel approach to stopping the rise of webcam child sex tourism', Terre des Hommes, 2013, p. 11.

142 Ibid., p. 12.

143 Livingstone, Sonia, Lucyna Kirwil, Cristina Ponte and Elisabeth Staksrud with the EU Kids Online Network, *In Their Own words: What bothers children online?*, LSE and EU Kids Online, 2013, p. 8.

144 UN Commission on Crime Prevention and Criminal Justice, 'Prevention, protection and international cooperation against the use of new information technologies to abuse

Although in some cases the victim may not know the identity of the perpetrator, a study carried out by Chicos.net, ECPAT International and Save the Children in Argentina suggests that aggression among peers is more frequent among children and adolescents who know each other from school or the neighbourhood. It also finds that this in turn affects face-to-face relations, generating fear and distrust. The role of bystanders is significant in all forms of bullying. Frequently, peers of a victim of cyberbullying remain silent and neither protest nor report the situation, whether out of fear or for other motives.[145]

Research is beginning to offer a greater understanding of the extent and nature of cyberbullying. Child Helpline International, a network of government and civil society organizations operating 173 child helplines in 142 countries around the world, began collecting data on cyberbullying in 2011, and by the end of 2012 had received more than 27,000 contacts about the issue. It notes that the number of boys contacting helplines about cyberbullying is slightly lower than the number of girls.[146]

The Cyberbullying Research Center, on the basis of its own research together with an extensive survey of articles published in peer-reviewed academic journals, concludes that about one out of every four teenagers in the United States has experienced cyberbullying, and about one out of every six teenagers has done it to others. Despite these figures, the Center suggests that traditional bullying is still more common in the country than cyberbullying. The Center's findings also suggest that adolescent girls in the United States are just as likely as boys (if not more likely) to experience cyberbullying, as either a victim or an offender.[147]

The EU Kids Online initiative also investigated online bullying. Of the sample group of 25,000 children aged 9 to 16, 6 per cent indicated they had been bullied online and 3 per cent admitted to having bullied others.[148] Recent data for selected European countries from the Net Children Go Mobile initiative indicate a higher incidence of cyberbullying (as well as of all online risks) than found by EU Kids Online. According to this research 10 per cent of children had been bullied face to face, while 12 per cent reported being bullied online or through mobile communication. This suggests that offline bullying may no longer be the dominant form of this behaviour.[149]

The most common technologies for cyberbullying were social networking sites (7 per cent of children in the preceding 12 months), SMS and texts (3 per cent), phone calls (2 per cent), instant messaging (2 per cent) and gaming websites (2 per cent). The research found notable differences according to age: the youngest children (9 to 10 years) are more likely to report being bullied face to face and on gaming websites, while cyberbullying among teenagers (aged 13-16) is more likely to occur on social networking sites.[150]

In the case of bullying, roles can be fluid. According to EU Kids Online, 60 per cent of those who bully, either online or offline, have themselves been bullied by others, while 40 per cent of those who bully online have also been the victims of bullying online.[151]

and/or exploit children. Report of the Secretary-General', E/CN.15/2014/7, 5 March 2014, §32.

145 Chicos.net, ECPAT and Save the Children Sweden, 'Chic@s y Tecnologías, usos y costumbres de niñas, niños y adolescentes en relación a las Tecnologías de la Información y la Comunicación', Chicos.net, ECPAT and Save the Children Sweden, 2009, p. 45.

146 It should be noted, however, that nearly 90 per cent of the children and young people contacting child helplines about cyberbullying hesitated to disclose their gender to protect their identity and maintain their anonymity after having suffered online abuse. Child Helpline International, 'Briefing paper on bullying', n.d. (circa 2013), p. 3, retrieved 18 March 2014 from <www.childhelplineinternational.org/media/57468/chi_briefing_paper_bullying.pdf>.

147 Cyberbullying Research Center, 'Cyberbullying Facts', retrieved 21 May 2014 from <www.cyberbullying.us/research/facts/>.

148 Livingstone, Sonia, et al., *EU Kids Online II, Final Report*, op. cit.,p. 24.

149 Mascheroni, G. and K. Ólafsson, *Net Children Go Mobile: Risks and opportunities*, second edition, Educatt, 2014, p. 63.

150 Ibid.

151 EU Kids Online, cited in 'The role of child protection systems in protecting children from bullying and cyberbully-

In the study of young people's use of MXit in South Africa, 26 per cent of respondents reportedly experienced insults on this social media platform. Of those who experienced insults, 28 per cent reported them to be race-based.[152]

The UNICEF study of young people in Kenya found that receiving hateful messages online, calling each other hurtful names or inappropriate posts on social media platforms were prevalent, although the term 'cyberbullying' was not used to describe this phenomenon. This was also the case in the South Africa study.

Regarding its impact, cyberbullying—like other forms of online risks—can affect different children in different ways depending on the available mechanisms of protection (such as effective anti-bullying policies in school), the personal strategies employed to tackle the issue and the degree of support received from friends, siblings, parents, teachers or other trusted persons.[153] It is thought that children and young people who are bullied online are more likely than victims of traditional bullying to have social problems, leading to general psychological distress and poor psychosocial adjustment.[154] The Cyberbullying Research Center suggests that cyberbullying is related to low self-esteem, anger, frustration and a variety of other emotional and psychological problems.[155] In extreme situations, cyberbullying has led to the victim's suicide or attempted suicide.[156]

Findings from EU Kids Online indicate that being bullied online by receiving nasty or hurtful messages is the least common Internet risk, but is most likely to upset children.[157] Of those children and young people who have been bullied online, 31 per cent reported that they were "very upset", 54 per cent were "fairly" or "a bit" upset, and only 15 per cent were "not upset at all".[158] Findings also suggest that girls are more upset than boys by bullying.

In terms of responses to cyberbullying, EU Kids Online found that most children who had received bullying messages online called on social support. One quarter, however, indicated they had not informed anyone. Six out of ten children had also used online strategies such as deleting hurtful messages or blocking the bully.[159] In Kenya, it was found that young people often react to these messages by simply deleting them, or 'unfriending' contacts who send or post such messages via social media. Young male participants in the Kenyan study often said that they reply with equally hurtful messages.[160]

Finally, research is beginning to throw light on another dimension of cyberbullying: children sending themselves anonymous bullying messages. A 2013 report from the Massachusetts Aggression Reduction Centre in the United States found that, of 617 students interviewed, 9 per cent had used social media for this purpose. In some cases, young people post messages about themselves that confirm their own insecurities, while others post personal questions online with the specific intention of receiving negative or abusive responses. Motivations for this behaviour are thought to

ing', background paper, *8th European Forum on the Rights of the Child*, Brussels, 17-18 December 2013, p. 4.

152 Beger, Gerrit, Priscillia Kounkou Hoveyda and Akshay Sinha, 'From 'What's your ASLR' to 'Do You Wanna Go Private?'', Digital Citizenship Safety/UNICEF, June 2011, p 12.

153 Donoso, Verónica and Eva Lievens, 'Participatory policy-making as a mechanism to increase the effectiveness of school policies against cyberbullying', synthesis report D.1.3.1 (incl. D.1.3.2), EMSOC, December 2013, p. 6. EMSOC stands for Empowerment in a Social Media Culture

154 UNICEF, 'Child Safety Online. Global challenges and strategies. Technical report', 2012, p. 44.

155 Cyberbullying Research Center, 'Cyberbullying Facts', retrieved 21 May 2014 from <www.cyberbullying.us/research/facts/>.

156 See, for example, 'Deaths associated with cyber bullying' in Golda Arthur, 'Rehtaeh Parsons: Father of cyberbully victim speaks out', *BBC News*, retrieved 1 April 2014 from <www.bbc.com/news/magazine-26723618>.

157 Livingstone, S., L. Haddon, A. Görzig and K. Ólafsson, 'Risks and Safety on the Internet: The perspective of European children. Initial findings', LSE and EU Kids Online, 2010, p. 11.

158 Livingstone, Sonia, et al., *EU Kids Online II, Final Report*, op. cit., p. 25.

159 RedNATIC, 'Estado de situaciòn sobre el derecho de la niñez y la adolescencia al uso seguro y responsible de las TIC en 10 países de América Latina', draft version, p. 4.

160 UNICEF, *A (Private) Public Space. Examining the use and impact of digital and social media among adolescents in Kenya*, UNICEF, 2013, p. 3.

include a 'cry for help' and for attention from adults and peers.[161]

4.6. Self-exposure

Sometimes the Internet contains photos that are put there without the person's consent [...].

15-year-old boy, Belgium[162]

The phenomenon of 'sexting'—that is, sending explicit self-generated text messages or images by mobile phone or instant messenger—is now widespread. In some cases young people, girls in particular, produce sexually explicit material as a result of peer pressure. In other cases it may be part of an 'intimate' online interaction. In both scenarios, there is a real risk of the material being viewed by people for whom it was not intended. Research findings from the Internet Watch Foundation suggest that up to 88 per cent of self-generated sexually explicit content online has been taken from its original location and uploaded elsewhere on the Internet.[163] In some cases, when material of this kind falls into the wrong hands, it can be used to blackmail children and young people into engaging in further risky behaviour, a criminal strategy commonly referred to as 'sextortion'.

There are many explanations for dissemination of images intended for private consumption. In some cases, there may be an explicit wish to cause harm to the individual in question. In others these images may be made available on impulse, because those involved are unaware of the implications of their actions, or because the perceived anonymity of the online environment encourages adolescents to act in ways they would not in face-to-face interactions. Once online, it is difficult, if not impossible, to eradicate suggestive or explicit material.

4.7. Children's involvement in cybercrime

Another emerging concern is the association of children and adolescents with cybercrime. This may include young men's engagement in computer-related financial fraud or the use of ICTs to facilitate illicit behaviour that may result in violence against themselves or others. For example, in the context of youth gangs, sexual images exchanged on mobile phones may become 'currency' for gang members, and mobile phones can be used to exert control over others and commission violent acts, including sexual violence. [164]

The Committee on the Rights of the Child, in its General Comment No. 13 on the right of the child to freedom from all forms of violence, acknowledges that children may become involved in "creating and uploading inappropriate sexual material, providing misleading information or advice, and/or illegal downloading, hacking, gambling, financial scams and/or terrorism."[165]

Information is still sparse on children's involvement in online sexual abuse and exploitation. In a study of adolescent male sexual abuse, researchers found that male offenders exhibited relatively high levels of drug and alcohol abuse, conduct problems and histories of delinquency. Female adolescent sexual abusers are thought to represent only 5 to 10 per cent of all juvenile abusers. They do, however, tend to choose younger victims and to be involved more often in incidents with multiple victims. The UN Special Rapporteur on the sale of children, child prostitution and child pornography has also drawn attention to the disturbing trend of self-produced, explicit sexual images produced by children themselves. Responses to these challenges must address the young person's behaviour and emphasize support and protection while avoiding stigma.

---

161 Winterman, Denise, 'Cyber self-harm: Why do people troll themselves online?', *BBC News Magazine*, 3 December 2013, retrieved 3 March 2014 from <www.bbc.com/news/magazine-25120783>.

162 Livingstone, Sonia, et al. *In Their Own Words* op. cit., p. 6.

163 Reported in UN Commission on Crime Prevention and Criminal Justice, 'Prevention, protection and international cooperation against the use of new information technologies to abuse and/or exploit children. Report of the Secretary-General', E/CN.15/2014/7, 5 March 2014, §36.

164 Information provided by Steven Malby, Senior Expert, Division of Treaty Affairs, Organized Crime and Illicit Trafficking Branch, UNODC, 23 May, 2014.

165 UN Committee on the Rights of the Child, General Comment No. 13 (2011). The right of the child to freedom from all forms of violence, CRC/C/GC/13, 18 April 2011, §31(c)(iii).

With the increasing engagement of organized criminal groups in cybercrime activities, there is a real risk of young people being drawn into online criminal activities, driven by bravado, attracted by promises of economic gain or compelled by threats or coercion.

4.8. Other concerns

A child can easily buy things behind his/her parents' back that they did not permit to buy.

14-year-old girl, Poland[166]

Harm to children may result, in addition, from obsessive online behaviour or excessive use of the Internet, which may in turn have a deleterious effect on their health or social skills. Children and young people may, for example, engage in informal games online that can, partly as a result of peer pressure, lead to psychological or physical harm. One example is the 'neknominate' online drinking game in which participants record themselves partaking in a physically extreme activity after chugging alcoholic beverages. This phenomenon, which attracted considerable public attention in early 2014 when it was reported to have gone 'viral' on Facebook, has been linked to a number of deaths.[167]

Deaths have likewise been associated with the *jeu du foulard,* also known as 'space monkey', a game that involves hyperventilating or squeezing the carotid artery in the neck to achieve a high. The popularity of this game among young people is largely due to videos of voluntary strangulation posted by teenagers on social media and video streaming sites.[168] In 2011, a study of 13,000 French school pupils between the ages of 7 and 13 found that 10 per cent of these children had participated in the *jeu du foulard*.[169]

Children are also known to make purchases online, enter agreements, sign up for premium services or make other forms of payments without the knowledge of parents of caregivers. In some cases this is a result of inappropriate or abusive online advertising directly aimed at this young audience.

Furthermore, children are vulnerable to online viruses, malware, worms, phishing and other risks that constitute threats to their privacy and safety and can also destroy their computers and devices. They may also be exposed to online fraud since, depending upon their level of maturity, they may be unable to distinguish legitimate requests from fraudulent ones. Fraudsters can use knowledge gained from children online to steal, blackmail, terrorize or even kidnap.[170] There are also cases (although rare) of individuals posting emotional pleas on social media platforms to track down partners or children who are, in fact, living under protection to escape domestic violence or abuse.

166 Livingstone, Sonia, et al., *In Their Own Words*, op. cit., p. 4.

167 See, for example, 'Neknomination: Warning issued in Orkney after hospitalization', *BBC News*, 12 February 2014, retrieved 22 May 2014 from <www.bbc.com/news/uk-scotland-north-east-orkney-shetland-26151273>. This article mentions incidents of students believed to be as young as 14 posting their own drinking videos online.

168 Judd, Terri, 'Teenagers risk death in internet strangling craze', *The Independent*, 6 January 2010, retrieved 11 July 2014 from <www.independent.co.uk/news/uk/home-news/teenagers-risk-death-in-internet-strangling-craze-1858987.html>.

169 Observatoire International de al Violence à l'Ecole, *À l'École des Enfants Heureux… Enfin Presque*, Observatoire International de al Violence à l'Ecole/UNICEF France, 2011, p. 21.

170 ITU, 'What's Happening Online', retrieved 25 October 2013 from <www.itu.int/osg/csd/cybersecurity/gca/cop/happening.html>.

5. Demographic, social and economic dimensions of violence against children

Child victims of violence, whether online or offline, tend to come from all walks of life. At the same time, characteristics such as age, gender, degree of vulnerability and geographic location can have an important bearing on children's online activities, the likelihood of their encountering certain kinds of risk, their reaction to these risks and their capacity for resilience.[171]

5.1. Age

Different age groups experience online harm in different ways and are also targeted in different ways. Younger children may be particularly vulnerable online because they lack technical expertise and the capacity to identify possible risks.

According to ECPAT International a considerable proportion of the victims of Internet-related sexual crimes are children under 12 years of age.[172] Recent figures from the Internet Watch Foundation suggest that as many as 81 per cent of victims in known child sexual abuse images are 10 or younger, and 3 per cent are 2 years of age or younger. This figure is up from 74 per cent in 2011.[173]

Findings from Europe suggest that as children get older, their experience of the Internet and their ways of interacting with it change and develop. Indeed, research indicates that children's concern with risks rises markedly between the ages of 9 and 12. This is supported by recent data from selected European countries for children aged 9 to 16, which suggest that the youngest children, aged 9 to 10, are the least likely to have been bothered by something online (11 per cent) compared with 23 per cent for children aged 15 to 16.[174]

Younger children are particularly concerned about risks related to the online content they might encounter, but as they get older, they become more concerned by conduct and contact risks, linked in many children's minds to the use of social networking sites.[175] Young adults are the primary targets of sex offenders who use the Internet to groom victims and meet them offline.[176] This suggests, in turn, that responses to this kind of risk must address the issues that cause certain young people to engage with adults online even when they are aware of the potential risks involved. Adolescents may also face unusually high risks of exposure to harmful material and cyberbullying.[177] It is reported that the vast majority of victims of bullying are 12 to 17 years old.[178]

171 d'Haenens, Leen, Sofie Vandoninck and Verónica Donoso, 'How to Cope and Build Online Resilience', EU Kids Online, January 2013, retrieved 26 June 2014 from <http://eprints.lse.ac.uk/48115/>.

172 ECPAT International, *Research Findings on Child Abuse Images and Sexual Exploitation of Children Online*, ECPAT International, September 2009, p. 4.

173 Figures cited in UN Commission on Crime Prevention and Criminal Justice, 'Study facilitating the identification, description and evaluation of the effects of new information technologies on the abuse and exploitation of children', 7 May, 2014, E/CN.15/2014/CRP.1, p. 126.

174 Mascheroni, G. and K. Ólafsson, *Net Children Go Mobile: Risks and opportunities*, second edition, Educatt, 2014, p. 59.

175 Livingstone, Sonia, et al., *In Their Own Words,* op. cit., p. 1.

176 Wolak, Janis, 'Research Findings in the United States about Sexual Exploitation via Virtual Interactions', pp. 6-9 of ECPAT International, *Research Findings on Child Abuse Images and Sexual Exploitation of Children Online*, ECPAT International, September 2009, p. 7.

177 UN Commission on Crime Prevention and Criminal Justice, 'Prevention, protection and international cooperation against the use of new information technologies to abuse and/or exploit children. Report of the Secretary-General', E/CN.15/2014/7, 5 March 2014, ¶40.

178 UN Commission on Crime Prevention and Criminal Justice, 'Study facilitating the identification, description and evaluation of the effects of new information technologies on the abuse and exploitation of children', 7 May, 2014, E/CN.15/2014/CRP.1, p. 26.

Pushing boundaries, exploring new experiences beyond adult scrutiny and testing one's capacities to cope with adversity are common characteristics of adolescence. These factors are important in shaping adolescents' online behaviour, and they must be taken into account when developing appropriate responses to online risks. Similarly, these responses must reflect and recognize the online protective strategies adopted by young people. They are, for example, often more likely to turn to an online or offline friend for help when they encounter disturbing situations than they are to consult with their parents.[179]

Generally, the older children get and the more experienced they become, the safer they are online. This suggests that it is particularly important to find ways to protect and empower younger children.

5.2. Gender

Gender differences also influence how children perceive and respond to online risk. Research from Europe indicates that boys appear more bothered by online violence than girls, while girls are more concerned with contact-related risks,[180] and teenage girls are slightly more likely to receive nasty or hurtful messages online than teenage boys.[181]

Boys and girls appear to be equally troubled about pornographic content. Slightly more girls than boys (41 per cent compared to 37 per cent) expressed concern about online risks associated with children their age, the EU Kids Online survey found. Although boys and girls encounter risks online in similar numbers, girls are more likely to be upset by them.[182] Some of the most recent data from Europe, collected by the Net Children Go Mobile project, indicate that among children aged 9 to 16, girls are significantly more likely to be bothered by an online experience than boys (21 per cent of the girls surveyed, compared to 14 per cent of the boys).[183]

There are also indications from Europe that boys enjoy more and better quality access to the Internet than girls.[184] This pattern is likely to exist in other regions, and especially in contexts where girls consistently experience greater discrimination in society than boys. A study by Plan International underlines the critical importance of ICTs for adolescent girls in terms of obtaining information; keeping connected; participating in social, political and cultural life; empowering themselves economically; and generally overcoming isolation in societies where their freedom and mobility is curbed at the onset of puberty.[185]

5.3. Vulnerability

Research suggests that youth who face challenges in their daily lives are also at risk of encountering problems online. Children belonging to vulnerable groups—including those of lower socioeconomic status, children affected by migration, children out of school, children belonging to minorities and children with disabilities—may be less likely to enjoy the benefits offered by the online environment or to receive information regarding online safety than their peers.[186] They may also be more likely to face bullying, harassment or exploitation online. Another subject for concern are higher risk youth, including those with histories of sexual abuse, family dysfunction, questions about their sexual orientation or patterns of online and offline risk taking.

179 UNICEF, 'Child Safety Online. Global challenges and strategies. Technical report', 2012, p. 15.

180 Livingstone, Sonia, et al., *In Their Own Words,* op. cit., p. 1.

181 Livingstone, S., L. Haddon, A. Görzig and K. Ólafsson, *Risks and Safety on the Internet: The perspective of European children. Full findings.* LSE and EU Kids Online, 2011, table 19, p. 62.

182 Livingstone, Sonia, et al., *In Their Own Words,* op. cit., p. 9.

183 Mascheroni, G. and K. Ólafsson, *Net Children Go Mobile: Risks and opportunities*, second edition, Educatt, 2014, p. 60.

184 Barbovschi, Monica and Michael Dreier, 'Vulnerable groups of children', ECPAT International, *Research Findings on Child Abuse Images and Sexual Exploitation of Children Online*, ECPAT International, September 2009, p. 60.

185 Bachan, Keshet, Sarah Stevenson and Nikki van der Gaag, 'Girls in Cyberspace: Dangers and opportunities', Plan International, n.d. (circa 2010), pp. 5-8.

186 On the other hand, research by Net Children Go Mobile in Europe has found that children from lower income families are the least likely to have experienced anything on the Internet that bothered them. See G. Mascheroni and K. Ólafsson, *Net Children Go Mobile: Risks and opportunities*, second edition, Educatt, 2014, p. 59.

Social isolation further affects the nature of a child's online behaviour and the amount of online activity, as well as his or her propensity to seek help when problems arise.[187] The likelihood of reporting concerns to the authorities is still lower in situations where young people lack confidence in the police, or where police officers themselves are perceived to lack the knowledge and background necessary to act in a child-sensitive manner and to effectively address crimes associated with new technologies. This calls for both technical training of police officers and the introduction of child-centred protocols that specifically address the situation of isolated or otherwise at-risk children.

Furthermore, socially isolated children and adolescents may be more likely to share sensitive information publicly. In some cases, this may include inappropriate or sexually explicit material, with a view to gaining acceptance and attention.[188] This has led researchers to identify a 'double jeopardy' effect, whereby children with more psychological problems suffer greater harm from both online and offline risks.[189]

Indeed, the Internet has the potential to compound and magnify existing vulnerabilities of certain children and young people and add to challenges they face in the offline world. In particular, the Internet has opened up a digital divide among children and young people, both between those who have ready and convenient access to the Internet at home, school and elsewhere and those who do not; and between those who are confident and proficient users of the Internet and those who are not. Without decisive interventions to extend quality Internet access to all children, this divide threatens to reinforce or exacerbate patterns of disadvantage.

At the same time, ICTs and the Internet have an enormous potential to overcome many of the challenges vulnerable children face in the offline world. Similarly, online participation, especially by means of social networks, offers a valuable means to overcome or reduce social isolation.

This is the case, for example, for children with disabilities and others who are more likely to encounter discrimination in face-to-face social interaction or experience difficulties interacting or communicating with their peers in an offline environment.

Despite this potential, many children with disabilities do not enjoy all or even some of the benefits ICTs bring. A 2013 report on this issue published by the ITU lists four key obstacles faced by children with disabilities: cost of assistive technologies; lack of access to ICT accessibility technologies; lack of policies (and of their effective implementation) that would foster widespread availability of accessible ICTs; and limited availability and use of ICTs.[190] To this list of challenges, which emphasizes economic and physical barriers, one can also add the deep discrimination and marginalization experienced by children with disabilities and their families around the world. This includes a lack of opportunities compared to their non-disabled peers, the extreme poverty in which many children with disabilities live and their social and political invisibility.

For young people at risk of discrimination on the basis of their sexual orientation, ICT use and online activity can help to overcome isolation and reach out, in safe online spaces, to social contacts and resources that can offer support and information. On the other hand, these young people may also face a serious risk of becoming victims of harassment online while being less likely to report incidents of cyberbullying to their parents or guardians. [191]

[187] UN Commission on Crime Prevention and Criminal Justice, 'Prevention, protection and international cooperation against the use of new information technologies to abuse and/or exploit children. Report of the Secretary-General', E/CN.15/2014/7, 5 March 2014, §40.

[188] UN Commission on Crime Prevention and Criminal Justice, 'Study facilitating the identification, description and evaluation of the effects of new information technologies on the abuse and exploitation of children, 7 May, 2014, E/CN.15/2014/CRP.1, p. 28.

[189] d'Haenens, Leen, Sofie Vandoninck and Verónica Donoso, 'How to cope and build online resilience?', EU Kids Online, January 2013, p. 1.

[190] Broadband Commission for Digital Development, Global Initiative for Inclusive Information and Communication Technologies (G3ict), the International Disability Alliance, ITU, Microsoft, Telecentre.org Foundation and UNESCO, *The ICT Opportunity for a Disability-Inclusive Development Framework*, ITU, September 2013, pp. 18-20.

[191] Blumenfeld, Warren J. and R.M. Cooper, 'LGBT and Allied Youth Responses to Cyberbullying: Policy implications',

5.4. Geographical considerations

Although the Internet by definition overcomes spatial barriers, geography plays an important role in influencing children's online experience. In addition, significant national and regional variations and preferences regarding Internet use and social media persist. As a result, the opportunity for children to become empowered digital citizens is conditioned by their place of residence, and higher prices in less developed areas only exacerbate the digital divide.[192]

Widespread poverty and weak State structures undermine social and legal protection for children and enhance the vulnerability of potential victims. In poorer countries children who have access to the Internet may be particularly vulnerable to online solicitation because their economic situation may pressure them into accepting propositions that include payment.[193] At the same time, parental knowledge and awareness of the online risks their children face might be lacking in these countries, effectively removing an important source of support and protection for children.

In industrialized countries and advanced East Asian economies, much of children's Internet access is from home: as many as 97.2 per cent of South Koreans, 84.8 per cent of Singaporeans and 81.3 per cent of Japanese have Internet access at home.[194] Increasingly, children are accessing the Internet from their own rooms or from mobile devices, a factor that further complicates parental supervision of children's Internet use. In developing countries, children and young people are more likely to access the Internet at school, on mobile phones or from Internet cafes. Where such cafes are unregulated or inadequately supervised, there is a greater risk that children will encounter inappropriate online material or fall victim to offline solicitation or abuse by customers, staff or owners. In a survey conducted by Plan International in Brazil, children indicated that risks in badly managed 'lan houses' (Internet cafes) include drug dealing and contact with and attention from unknown adults. [195]

Underdeveloped regulatory frameworks can heighten the potential online risks to children and increase their exposure to harm. As noted by UNICEF, gaps in online protection may be greater in low- and middle-income countries, where gaps in overall child protection already exist. Although much remains to be understood about the behaviour of children and young people online and the most effective protection responses, it is clear that children are less confident about keeping safe in countries where online safety information is not widely available.[196] Given this, and the dramatic increase in Internet access, broadband uptake and mobile-cellular subscriptions in the developing world, it is likely that some of the greatest challenges to ensuring children's online safety in coming years will arise in lower-income countries.

International Journal of Critical Pedagogy, vol. 3(1), 2010, pp. 114-133, pp. 122-123.

192 Ibid., p. 8.

193 Ibid., pp. 35-36.

194 ITU data cited in 'Data Chart ASIA—World Bank-ICMEC Desk Review Project'.

195 Bachan, Keshet, Sarah Stevenson and Nikki van der Gaag, 'Girls in Cyberspace: Dangers and opportunities', Plan International, n.d. (circa 2010), p. 13

196 UNICEF, 'Child Safety Online. Global challenges and strategies. Technical report', UNICEF, 2012, p. 45.

6. A multifaceted agenda for releasing children's potential and minimizing online risks

As underscored in the previous sections, the challenge of creating a safe and empowering online environment for children lies in responses that strike the appropriate balance between ensuring that children benefit from the potential offered by ICTs and securing their necessary protection.

Clearly, the multidimensional nature of violence requires a multifaceted response. It calls for concerted prevention initiatives, respect for and fulfilment of children's rights at all times, detection of offences, appropriate criminal justice responses to fight impunity, provision of effective remedies and assistance to victims, including for their rehabilitation and reintegration. In addition after-care is needed for perpetrators of sexual abuse offences.

As described in this section, consolidating progress in this fast-changing area requires pursuing a multifaceted agenda and capitalizing on the potential of strategic partnerships. National authorities, families, schools, civil society and the corporate sector are key actors in this process, and the child's best interests and children's active contribution to their own protection need to be at the heart of these efforts.

6.1. Empowering children and young people

Online safety initiatives aimed at children, particularly adolescents, must recognize their crucial role in this process. Children master ICTs with ease, but they need skills and confidence. They also need to feel secure when they explore the borders of the digital universe and when they encounter issues of concern.

As young people stressed during the 2013 Global Youth Summit promoted by the ITU (see box 5),[197] it is important to go beyond simply trying to avoid online threats. Children need to develop their capacities as digital citizens and to learn solid values and life skills, including a strong sense of responsibility, respect and concern for others. Rather than curtailing children's natural curiosity and sense of innovation for fear of encountering risks online, it is critical to tap into children's resourcefulness and enhance their resilience while exploring the potential of the Internet.

Box 5.
BYND 2015: global youth call for child safety online

In September 2013, Costa Rica organized, in cooperation with the ITU, the Global Youth Summit: BYND 2015. This event convened young people to participate, both online and offline, in a discussion on the positive application of technology.

In the 'Be Safe Be Smart' session, young people discussed risks related to the use of the Internet and social media, and about how they can communicate or raise awareness about these risks. A train-the-trainer initiative taught young people how to use an online safety training kit to help younger children use the Internet safely and responsibly. The summit included a global competition among young people who developed concepts for videos related to online safety.

At the end of the summit, the young participants adopted a Global Youth Declaration.

Source: www.itu.int/en/bynd2015/Pages/defaultold.aspx

A positive, caring and protective family environment, a supportive community environment, access to relevant and child-friendly information and services, including tools for reporting online abuse, are crucial factors to achieve this goal, in parallel with children's own evolving capacities.

[197] www.itu.int/en/bynd2015/Pages/be-smart-be-safe.aspx.

Children and young people want to be able to navigate the online world in safety. This ambition is reflected in many initiatives, including the Manifesto developed by more than 1,000 teenagers from Latin America during national forums, along with a regional online awareness raising campaign—*Todo a 1 Clic*—to promote safer Internet use.

The Committee on the Rights of the Child has emphasized the importance of educational measures for children to prevent and address violence, with a view to ensuring the "provision of accurate, accessible and age-appropriate information and empowerment on life skills, self-protection and specific risks, including those relating to ICTs and how to develop positive peer relationships and combat bullying".[198]

Developing the online competence of children and adolescents must also include building their capacities as digital citizens based on solid values and life skills, not just avoiding the risk of specific online threats. This involves focusing action on individuals and their attitudes more than the specific technologies they use. It also requires that everyone using ICTs, including children and adolescents, must recognize themselves as rights-holders who must simultaneously demonstrate responsibility, respect and concern for others.[199] This shift is reflected, for example, in a new emphasis in EU policy not just on developing a safer Internet but also on creating a better Internet for children.[200]

Children are far from passive when it comes to their online safety. Research has shown they are capable of developing strategies to deal with negative experiences, such as blocking insulting contacts and withholding personal details;[201] finding safety advice online; changing privacy settings on a social networking profile; comparing websites to judge their quality or block spam.[202]

The potential of children to address their own protection concerns is closely associated with their evolving capacities. The fact that some children and young people adopt new technology with ease does not mean they do not require support, information and guidance on protection strategies in order to remain safe. Nor does it remove the necessity of effective protection measures and law enforcement. Children of every age should have a means of contacting child-friendly services or other forms of support.

Given that curiosity is normal and healthy, adolescents need information about the risks and dangers of online contact, in particular with adults. Children must be informed in an age-appropriate and child-friendly manner of how to report threatening or inappropriate interactions and violence and the likely process that may follow. This requires the establishment of counselling, complaint and reporting mechanisms that are widely available, easily accessible, child-sensitive and confidential.

For children under age 9, the onus for ensuring protection lies primarily with parents, caregivers, teachers and other qualified professionals. Given the significance of a child's age in how the Internet and ICT devices are used and risks are experienced, significant efforts have been promoted by various groups with tailor-made recommendations for children of various age groups and for parents and teachers, as in the case of the ITU, EU Kids Online[203] and the 'thinkuknow' websites, developed in the UK by CEOP (see box 6). Targeted and tailored prevention strategies are equally required for the most vulnerable or at-risk youth populations, including children belonging to minorities and children with disabilities.

198 UN Committee on the Rights of the Child, General Comment No. 13 (2011). The right of the child to freedom from all forms of violence, CRC/C/GC/13, 18 April 2011, §44(b).

199 RedNATIC, 'Estado de situaciòn sobre el derecho de la niñez y la adolescencia al uso seguro y responsible de las TIC en 10 países de América Latina', draft version, p. 22.

200 See, for example, Brian O'Neill, Elisabeth Staksrud and Sharon McLaughlin, *Towards a Better Internet for Children? Policy pillars, players and paradoxes*, Nordicom, 2013.

201 Pawelczyk, Kate, 'Kenya study looks at the growing community of new Internet users', retrieved 28 October 2013 from <www.unicef.org/infobycountry/kenya_70525.html>.

202 Livingstone, S., L. Haddon, A. Görzig and K. Ólafsson, *Risks and Safety on the Internet: The perspective of European children. Initial findings.* LSE and EU Kids Online, p. 13.

203 Holloway, D., L. Green and S. Livingstone, *Zero to Eight. Young children and their internet use.* LSE and EU Kids Online, 2013, p. 5.

Box 6.
CEOP's age-specific thinkuknow websites

In the United Kingdom, the Child Exploitation and Online Protection Centre (CEOP) offers four 'thinkuknow' websites tailored to specific age groups, from 5 to 14-plus.

The language and design of each of the websites reflect the interests of the specific audience, as do the issues addressed. For children aged 5 to 7, the thinkuknow website includes cartoon graphics and simple games: "If you are 5, 6 or 7, I bet you probably like to use the computer for fun. We've made this website to help you go on the Internet in a safe way and know who to talk to if you are worried."

In contrast, the website for adolescents presents an 'edgy' graphic and includes many photographic images of adolescent social interaction. The homepage includes a number of short videos addressing specific issues of concern, including self-exposure, cyberbullying and offline meetings with online contacts. Importantly it also explains what to do and where to go to get help, and it includes resources for parents and carers, and teachers and trainers.

In a number of countries, children and young people can benefit from information, advice and support from national children's ombudspersons offices, to whom they also can report violence-related concerns. Many of these offices—which ideally are independent and autonomous—can receive and investigate complaints from both children and adults about a range of organizations and services influencing children's well-being and the enjoyment of their rights.

Another concern is children's ability to remove their traces from the Internet, and their right to do so has been widely discussed. In May 2014, the European Court ruled that Google and other search engines must listen and, when appropriate, comply when people ask for removal of links to newspaper articles or other sites containing outdated or otherwise objectionable information about themselves.[204] The Court's decision opens avenues for children to remove prejudicial or harmful material that relates to them. However, this measure is unlikely to have a significant impact on the illegal and covert circulation of child sexual abuse material.

For children who engage in online bullying and harassment or are involved in cybercrime, restorative justice models are needed to encourage them to take responsibility for their actions and change their behaviour. Restorative justice offers an important means of addressing the harm caused by an offence rather than focussing on punishing it, thus constituting an important measure for promoting a sense of accountability while avoiding children's criminalization.

Restorative justice is voluntary and based on the agreement of both the offender and the victim to commit to a respectful and restorative process. Restorative justice can be achieved by a range of practical measures, which are set out in detail in *Promoting Restorative Justice for Children*, produced by the Office of the SRSG on Violence against Children.[205]

6.2. Supporting parents and caregivers

Informed and engaged parents or caregivers who share Internet experiences with their children encourage a safer online experience.[206] Parents' effective mediation minimizes risk without limiting children's skills or opportunities. Strategies include support for children's Internet use, guidance on safety and establishment of rules to regulate use.[207] However, findings suggest that children do not always see parents or caregivers as their first

[204] See, for example, 'European court: Google must yield on personal info', *Washington Post*, retrieved 22 May 2014 from <www.washingtonpost.com/world/europe/european-court-google-must-amend-some-results/2014/05/13/f372fe08-da78-11e3-a837-8835df6c12c4_story.html>.

[205] SRSG on Violence against Children, *Promoting Restorative Justice for Children*, Office of the SRSG on Violence against Children, 2013.

[206] UNICEF, 'Child Safety Online. Global challenges and strategies. Technical report', UNICEF, 2012, p. 45.

[207] Mascheroni, Giovanna, Maria Francesca Murru, Elena Aristodemou and Yiannis Laouris, 'Parents: Mediation, Self-regulation and Co-regulation', in Brian O'Neill, Elisabeth Staksrud and Sharon McLaughlin, *Towards a Better Internet for Children? Policy pillars, players and paradoxes*, Nordicom, 2013, p. 211.

resort in addressing concerns about online safety. The implications of this observation can be particularly significant in developing countries, where the digital gap between generations is often wide.

Parents and caregivers themselves must therefore be supported to better understand the online environment, how children and young people operate in it, the type of risks they might encounter, the harm that can potentially ensue and the most effective ways to avoid this harm and develop resilience among children and young people.

The ITU *Guidelines for Parents, Guardians and Educators on Child Online Protection*[208] offer practical approaches to online safety. These include steps to ensure the safety and security of computers in the home and establishment of rules on ICT use based on open discussion with children. Children need to be educated about safe and responsible online behaviour, including the importance of never arranging to meet anyone they first met online, preventing children from disclosing information that would allow them to be identified personally, ensuring children understand what it means to post photographs on the Internet and warning them about expressing feelings and emotions to strangers. [209]

The guidelines also underscore the importance of adults themselves becoming informed about risks and potential harm and learning about how their children use technology. They encourage parents and caregivers to explore the sites their children visit to be aware of the safety features these sites incorporate, the types of advertising they host, the degree of control they permit over credit card purchases and other means of payment, and the form of moderation employed, if at all. Filtering, blocking and monitoring programmes[210] can be useful for preventing younger children from accessing harmful and inappropriate content, but findings suggest that these tools are not widely known or used by parents.[211]

For older children, filtering or blocking may be less effective since much of the content that bothers older children is user-generated,[212] and most of these tools are only effective in the English language. In addition, there are few filtering and blocking tools suitable for games consoles, tablets and mobile phones, the devices increasingly used by children to go online.[213] These findings suggest that, as stressed in the previous section, it may be more effective to concentrate on raising children's awareness of online threats, informing them of the correct steps to take should they encounter such threats and working to improve their confidence and resilience online.[214]

6.3. Capitalizing on the potential of schools

Schools have a unique potential to promote non-violent behaviour and support change of attitudes condoning violence. Through quality education,

[208] ITU, *Guidelines for Parents, Guardians and Educators on Child Online Protection*, International Telecommunication Union, 2009, pp. 50-53.

[209] Ibid., p. 54.

[210] Filtering systems enforce certain predetermined filtering policies and evaluate whether a user can or cannot access specified material. Filtering software can be either server-side or client-side (or user-side), that is, installed on the servers of Internet content providers or ISPs, or installed by individuals on personal computers. Kim-Kwang Raymond Choo, 'Online Child Grooming: A literature review on the misuse of social networking sites for grooming children for sexual offences', Australian Institute of Criminology, AIC Reports, Research and Public Policy Series, no. 103, 2009, p. xvi.

[211] Livingstone, S., L. Haddon, A. Görzig and K. Ólafsson, with members of the EU Kids Online network, *Risks and Safety on the Internet. The perspective of European Children. Full findings*, 2011, cited in European Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. European Strategy for a Better Internet for Children', COM(2012) 196 final, Brussels, 2 May 2012, p. 11.

[212] Livingstone, Sonia, et al., *In Their Own Words,* op. cit., p. 14.

[213] European Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. European Strategy for a Better Internet for Children', COM(2012) 196 final, Brussels, 2 May 2012, p. 4.

[214] See, for example, Elisabeth Staksrud and Jørgen Kirksæther, 'Filtering & Content Classification', pp. 23-37 of Brian O'Neill, Elisabeth Staksrud and Sharon McLaughlin, *Towards a Better Internet for Children? Policy pillars, players and paradoxes*, Nordicom, 2013, p. 2.

children can also gain the skills and abilities to surf cyberspace with confidence, avoid and address risks, and become well-informed and responsible digital citizens. This includes promoting creative, critical and safe use of the Internet and preventing and responding to incidents of online violence. As the report of the SRSG on Violence against Children "*Tackling Violence in Schools: a global perspective, bridging the gap between standards and practice*" points out, schools represent, "important resources for the development and dissemination of values of non-violence, cooperation, tolerance and respect, not only among pupils and staff, but also beyond, in the wider community."[215]

Teachers and other school staff must be aware of the steps to take should they discover that a child has encountered a negative online situation. Even where lack of education resources precludes access to technology, it is still important for staff to teach children about ICTs and support them in learning to be constructive, resourceful and respectful online citizens.

Likewise, while incidents of cyberbullying many not necessarily originate in the school environment, schools have a central role in addressing this phenomenon. Not all children have the tools or the social or family support to deal with cyberbullying on their own. This makes it all the more important for schools to be well prepared to deal with this phenomenon and to help all the children involved (bullies, victims and bystanders) to cope in an effective and constructive way.[216] Ideally, responses to both online and offline bullying include a 'whole-school' approach and restorative ethos, guided by a coherent and consistent anti-bullying policy. These responses should involve all relevant actors, including students, teachers, administrative and auxiliary staff, parents and caregivers, and the community in which the school is located, as described in the SRSG Study mentioned above, "*Tackling Violence in Schools: A global perspective, bridging the gap between standards and practice*".[217]

A necessary precondition for any school-based initiative is for teachers themselves to understand the online environment and have the capacity to identify early signals of abuse, as well as to advise, guide, empower and support children and young people. Important initiatives are being promoted to this end, including the Intel Teach programme, which has trained more than 10 million teachers in over 70 countries to integrate technology into classrooms.[218]

Furthermore, teachers, sports coaches and other adults who work with children have a clear responsibility to maintain ethical standards in their own online interactions. For example, many teachers recognize the benefits of using ICTs and social media to communicate with their students. However, in some countries it is reported that social media have facilitated a number of unethical or abusive relationships between teachers and students, so caution is required.[219]

Promoting digital literacy in schools can also leverage efforts aimed at children's social inclusion. In addition it can narrow the digital divide affecting the most vulnerable children, who otherwise are less likely to enjoy the benefits of new technologies or access information promoting safe Internet use.

Ideally, the school serves as a bridge between a child's home and her or his community. It can serve as a place where students, parents and other community members meet to gain digital literacy and confidence and benefit from ICT-based training on life skills, social and economic empowerment, and entrepreneurship. Indeed, where computers and other devices are scarce and parental confidence

215 SRSG on Violence against Children, *Tackling Violence in Schools: A global perspective*, Office of the SRSG on Violence against Children, 2013, p. 2.

216 Donoso, Verónica and Eva Lievens, 'Participatory policy-making as a mechanism to increase the effectiveness of school policies against cyberbullying', Synthesis Report D.1.3.1 (incl. D.1.3.2), EMSOC, December 2013, p. 6.

217 SRSG on Violence against Children, *Tackling Violence in Schools: A global perspective*, Office of the SRSG on Violence against Children, 2013.

218 Glinski, Allison M., Ellen Weiss, Adithi Shetty with Gillian Gaynair, *Preparing Girls and Women for 21st Century Success: Intel teach findings*, International Center for Research on Women, 2013, p. 2.

219 For a fuller discussion of this issue in the United States, see Jennifer Preston, 'Rules to stop pupil and teacher from getting too social online', *New York Times*, 18 December 2011, pp. 1 and 4.

online is low, schools with computing facilities can provide digital literacy training to parents and other community members through evening classes or other means. This is the concept behind the Connect a School, Connect a Community initiative (see box 7).

Box 7.
Connect a school, connect a community

The Connect a School, Connect a Community is a public-private partnership launched by the ITU to promote broadband Internet connectivity for schools in developing countries. It is based on the concept that connected schools should cater not only for the children who attend them, but also for the broader communities in which these children live. In this way, schools can serve as community ICT centres for disadvantaged and vulnerable groups, including women and girls, indigenous peoples and persons with disabilities. Children and youth attending connected schools will have improved access to the latest ICTs, while community members will receive ICT-based training on basic life skills (language literacy, numeracy and basic ICT literacy) along with training that develops business and ICT-specialized skills.

6.4. Joining efforts with civil society

NGOs and other civil society organizations play a central role in protecting children online and responding to harm when it arises. Among their activities, they conduct awareness-raising campaigns, offer training and information, influence needed policy developments, provide support for child victims of violence and abuse, operate hotlines and helplines, and conduct much-needed research. Initiatives like make-IT-safe work to ensure the safety of children and young people online and in interactive technologies. This global campaign, led by ECPAT International and the Children's Charities Coalition for Internet Safety, adopts the strategy of engaging both the corporate and government IT sectors to deliver legal, technological and social solutions and financial resources, while engaging in awareness-raising activities (see box 8).

Box 8.
The make-IT-safe campaign

The make-IT-safe campaign aims to make new online technology safe for children and young people everywhere. It raises awareness about the dangers of online violence among adults and children, addressing attitudes that disregard the problem and beliefs that it is only an issue in other countries. It also empowers young people to promote Internet safety and encourages Internet cafes around the world to sign a code of conduct. The campaign, initiated in 2005, brings together children's groups in 67 countries and provides a range of mobilization and materials, including postcards, stickers, flyers and T-shirts.

For example, a postcard for display in Internet cafes, reads:

Use Internet safely:
Protect yourself from sexual exploitation

In our Cyber Café:

- We have specified areas in the cafe for use by children and youth.
- We discourage all viewing of pornographic images and pornographic websites.
- We keep a protective watch over children and youth who communicate online in the café and we offer our assistance if an unusual situation occurs.
- We advise children and youth not to trust anyone they meet online and to be wary of giving out personal information.
- We provide awareness-raising materials with information about young people's safety and protection issues.
- We will refer suspicious activities of potential abusers to child rights organizations or a hotline.
- We report or block all websites that we are aware of that contain sexual images of children, hate or racial content.

This and other resources are available from the make-IT-safe website: www.make-IT-safe.net.

Despite these significant initiatives, one important challenge faced by NGOs is the lack of broad societal understanding about how to define and recognize online risks, including violence, abuse and exploitation, or what steps to take to reduce the harm they may cause. There may also be a lack of awareness among the general public as to whether conduct such as cyberbullying and cyberharassment constitutes a criminal offence and to whom it should be reported. If major concerns such as these are not addressed in public campaigns, there is a real risk that these campaigns will only increase anxiety instead of achieving a preventive effect.[220]

Hotlines and helplines, often operated by civil society groups, are an essential element in making the Internet a safer place by offering the public a means of anonymously reporting online content they suspect to be illegal or harmful. INHOPE, which coordinates a network of 46 Internet hotlines in 40 countries, works to make the Internet safer by responding to reports of illegal content. It receives funding and support from the European Commission under the Safer Internet Programme.[221]

Whether by phone, email or instant messaging, helplines are often the first point of contact with children seeking assistance in connection with violence. Child Helpline International, present in more than 140 countries, registers more than 14 million calls a year from children and young people in need of care and protection. While many child telephone helplines were not established to address violence associated with ICTs, they must nevertheless have the structure and staff in place to deal with these important issues. Partnerships again offer a means to overcome the limitations and challenges that may be faced in this area.

Helplines are particularly valuable with respect to highly sensitive issues, such as sexual abuse, which children may find difficult to discuss with peers, parents, caregivers or teachers. Helplines also play a crucial role in directing children to services such as legal services, safe houses, law enforcement or rehabilitation, all of which should be an integral part of the national child protection system. Unfortunately, where the national child protection system does not have the capacity to respond to these requirements, helplines have had to provide these services themselves, by employing specialized staff. Some helplines may lack the capacity to respond to a call by providing adequate follow-up services, and where such services exist, they may not have the resources and skills to address children's concerns.

Given their outreach, there is a compelling argument for recognizing helplines as core components of integrated national systems of child protection and to ensure they receive necessary funding. The success of helplines will depend on what, if any, follow-up models they employ, their availability and cost, their geographic reach and the care taken to ensure that they are confidential and linked to law enforcement and other support services.

Finally, civil society organizations can and do play an important role in collecting data and promoting research on ICT use among children and young people. In the case of RedNATIC's virtual consultation with adolescents, *Exprésate Latinoamérica,* Costa Rica's *Fundación Paniamor* developed the consultation tool and took responsibility for compiling and analysing the results and identifying significant findings. Chicos.net, from Argentina, took responsibility for coordinating implementation of the consultation across nine countries, working with national organizations belonging to the RedNATIC network. These organizations in turn took direct responsibility for organizing the participation of adolescents in each country and administering the questionnaires. Technical and financial support was provided by Save the Children.[222] The

[220] National Rapporteur on Trafficking in Human Beings, *Child Pornography—First report of the Dutch National Rapporteur*, BNRM, 2011, p. 127.

[221] INSAFE-INHOPE,*INSAFE-INHOPE: Working Together for a Better Internet for Children and Young People. Annual report 2013*, 2014, retrieved 14 July 2014 from <www.inhope.org/Libraries/Annual_reports/Insafe_INHOPE_Annual_Report_2013.sflb.ashx>.

[222] RedNATIC, 'Estado de situaciòn sobre el derecho de la niñez y la adolescencia al uso seguro y responsible de las TIC en 10 países de América Latina', draft version, pp. 67-68.

result is a detailed and much-needed insight into the use of ICTs by children and adolescents in a significant section of the Latin American region.

6.5. Consolidating partnerships with the corporate sector

The corporate sector, an essential driver for societies and economies, can actively contribute to preventing violence, minimizing risks and securing online protection for children. This is particularly important given that their services or products can be used to expose children to online abuse, including violent content, cyberbullying and sexting, grooming and sexual abuse.

ISPs, social media companies and manufacturers and distributors of ICTs, and small businesses providing children access through Internet cafes, all have a crucial role to play in children's online protection and in fighting impunity. As an important content provider, the corporate sector also has a responsibility to provide quality, engaging and age-appropriate online content for children. A number of recent international developments reflect the significance of the corporate sector in this area:

- The UN Committee on the Rights of the Child has explicitly recognized the importance of collaboration with the mass media and the ICT industry to devise, promote and enforce global standards for child caregiving and protection.[223] In its General Comment no. 16 (2013), the Committee addresses State obligations regarding the impact of the business sector on children's rights. Recognizing the role of business in strengthening realization of children's rights, it notes that companies can be complicit in criminal acts involving violence against children through the Internet.[224]
- The responsibilities of the corporate sector to respect and promote human rights are clearly iterated in the Guiding Principles on Business and Human Rights, developed by the Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises, and endorsed by the UN Human Rights Council in 2011.
- The Children's Rights and Business Principles developed by UNICEF, the UN Global Compact and Save the Children are the first comprehensive set of principles to guide companies on the full range of actions they can take in the workplace, marketplace and community to respect and support children's rights.[225]
- The ITU has revised and further developed its Guidelines for Industry on Child Protection Online, in line with the Guiding Principles and together with UNICEF. They focus on how industry can integrate child rights into policy and management; processes for handling child sexual abuse material; the establishment of safe and age-appropriate online environments; online safety education for children, parents and teachers; and promoting the positive use of ICTs.[226]
- The Lanzarote Convention (the Council of Europe Convention on Protection of Children against Sexual Exploitation and Sexual Abuse), requests States to encourage the private sector to participate in elaborating and implementing policies to prevent sexual exploitation and sexual abuse of children and to implement internal norms through self-regulation or co-regulation. It also encourages cooperation between state authorities, civil society and the private sector to prevent and combat sexual exploitation and abuse of children, including through measures to hold individuals liable for offences.

The corporate sector can undertake a number of practical actions to secure children's online safety. The European Commission, in its 'European Strategy for a Better Internet for Children', makes a number of specific recommendations that are

[223] UN Committee on the Rights of the Child, General Comment No. 13 (2011). The right of the child to freedom from all forms of violence, CRC/C/GC/13, 18 April 2011, §43(a)(viii).

[224] UN Committee on the Rights of the Child, General Comment No. 16 (2013) on State obligations regarding the impact of the business sector on children's rights, CRC/C/GC/16, 17 April 2013, §60.

[225] See UNICEF, 'Introduction to the Principles', retrieved 12 March 2014 from <www.unicef.org/csr/12.htm>.

[226] The revised ITU Guidelines for Industry are forthcoming. See <www.itu.int/en/cop/Pages/guidelines.aspx>, retrieved 24 June 2014.

pertinent for industry in all regions of the world.[227] In brief, these recommendations are to:

- Promote positive online experiences for young children;
- Engage in private-public partnerships to support the development of digital and media literacy and teaching online safety in schools;
- Scale up awareness activities and youth participation;
- Introduce simple and robust reporting tools for users;
- Implement age-appropriate privacy settings, with clear information and warnings;
- Ensure wider availability and use of parental controls;
- Promote wider use of age rating and content classification;
- Address online advertising and overspending;
- Introduce faster and systematic identification of child sexual abuse material disseminated through various online channels and more rapid notification and removal of this material; and
- Pursue cooperation with international partners to fight child sexual abuse and exploitation.

The corporate sector can also provide much-needed technical support, training and equipment to law enforcement authorities to enable them to identify offenders, collect evidence required for criminal proceedings and adjust to the constantly evolving methods employed by criminals who use ICTs to commit crimes.[228] As noted by the UN Commission on Crime Prevention and Criminal Justice, forensic software is needed to collect evidence, conduct keystroke logging and decrypt or recover deleted files in investigations involving new ICTs.[229]

The potential of the corporate sector to contribute to child protection is illustrated by mobile phone operators' worldwide establishment of the Mobile Alliance against Child Sexual Abuse Content in 2008. Through a combination of technical measures, cooperation and information sharing, it works to obstruct the use of the mobile environment to consume or profit from child sexual abuse content.[230]

Promising as these developments may be, in such a fast-changing universe it remains essential to pursue effective implementation, periodic evaluation and further improvement of the framework developed so far, both to secure children's safety and to seize the potential of the digital world.

6.6. Building on States' accountability to secure children's online protection

Governments have a leading responsibility in the realization of children's rights. This includes violence prevention and children's online protection. Without the committed involvement of governments, it is significantly harder for other actors—including professionals working with and for children, the corporate sector and civil society organizations—to act confidently and effectively in this area.

Capitalizing on implementation of the recommendations of the UN Study on Violence against Children, the children's digital agenda should be integrated as a core component of the national comprehensive, well-coordinated and well-resourced policy framework to prevent and address all forms of violence against children. This agenda requires the involvement of all stakeholders and must be informed by the views and experiences of children and young people online, including those exposed to abuse.

227 European Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. European Strategy for a Better Internet for Children', COM(2012) 196 final, Brussels, 2 May 2012, pp. 7-15.

228 Commission on Crime Prevention and Criminal Justice, 'Discussion guide for the thematic discussion of protecting children in a digital age: the misuse of technology in the abuse and exploitation of children', 31 January 2011, E/CN.15/2011/2, §32.

229 Ibid.

230 See 'Mobile Alliance against Child Sexual Abuse Content', retrieved 7 March 2014 from <www.gsma.com/publicpolicy/wp-content/uploads/2013/10/GSMA_The-Mobile-Alliance-Against-Child-Sexual-Abuse-Content_Oct-2013_2ppWEB.pdf>.

National legislation is a core dimension of this process and is indispensable to enable children's enjoyment of digital literacy without discrimination and to ban all forms of violence in all settings, including cyberspace. It secures children's protection, providing for effective remedies, recovery and reintegration to address online harm, abuse or exploitation. Legislation also establishes child-sensitive counselling, reporting and complaint mechanisms and procedures, as well as accountability mechanisms to fight impunity.

Governments have a leading responsibility to bring their legislation into line with international child rights instruments. As highlighted by the Expert Consultation on Law Reform organized by the SRSG on violence against children in 2011, it is critical to establish a firm legal foundation to prevent all forms of violence against children and a dynamic legal response to new and emerging challenges. Enactment of laws needs to be matched by effective enforcement.

Legislation needs to be flexible to avoid constant updating, but it also needs to convey a clear prohibition of all manifestations of violence. The law needs to address loopholes associated with emerging concerns, including new forms of online abuse such as grooming, and develop procedural criminal proceedings to facilitate investigation and prosecution.

Significant legislative developments have addressed the protection of children from cyberbullying and from exploitation through pornographic materials.

The 2012 report on child pornography of the International Centre on Missing and Exploited Children (ICMEC) found that the number of countries deemed to have sufficient law had climbed from 27 in 2006 to 69 in 2012. Fifty one countries enacted legislation against child pornography for the first time, 49 passed legislation defining child pornography, 57 criminalized computer-facilitated offences, 47 criminalized simple possession of child pornography and 8 mandated reporting by ISPs. Yet 53 countries still had no law in this area.[231]

Box 9.
The Philippines Anti-Child Pornography Act of 2009

The Philippines Anti-Child Pornography Act lists prohibited and unlawful acts, which include hiring, inducing, persuading or coercing a child to perform in the creation or production of child pornography; producing, manufacturing or directing child pornography; offering, publishing, selling, distributing, broadcasting, promoting, importing or exporting child pornography; and possessing child pornography with the intention to sell, distribute or publish.

The law defines and prohibits grooming of children for sexual purposes and requires private sector actors, such as ISPs, private business establishments and Internet content hosts, to assist in the fight against child pornography. ISPs have the obligation to notify the Philippine National Police or the National Bureau of Investigation within seven days upon discovery that their servers or facilities are being used to commit child pornography offences. They are also obliged to preserve evidence for use in criminal proceedings. Upon request by law enforcement authorities, they must give details of users who access or attempt to access websites containing child pornography. ISPs must also install programmes or software designed to filter and block child pornography. Additionally, owners and operators and owners or lessors of other business establishments have the responsibility to report child pornography offences within seven days of discovering that their premises are being used to commit such offences.

Importantly, the Act also requires appropriate protections for child victims of pornography offences. This includes strict confidentiality in handling evidence, protecting witnesses and assisting in recovery and reintegration.

As understanding of the phenomenon of grooming and other preparatory acts in the process of the sexual exploitation of children has increased, countries are incrementally adding such offences to their laws. Notable among these are the provi-

[231] ICMEC, *Child Pornography: Model legislation & global review*, 7th edition, ICMEC, 2012, retrieved 8 November 2013 from <www.icmec.org/en_X1/icmec_publications/ICMEC_Highlights_2012.pdf>.

sions introduced in the Philippines under the Anti-Child Pornography Act of 2009, which includes measures to prevent and penalize grooming [232] (see box 9).

State accountability is equally important to set a clear regulatory framework for corporate activities and to support businesses in meeting their responsibilities to safeguard children's rights. Professionals working with and for children should benefit from capacity-building initiatives to gain skills and expertise on online risks children may face. This should include how to recognize early signals of abuse and the required steps to address them in an ethical and child-sensitive manner.

Comprehensive legislation provides the framework for the development of effective public policies. Government policies must explicitly address children's online safety and protection, while dovetailing with broader policies to prevent violence against children in general. Policy responses call for governments to incorporate measures addressing ICTs and the Internet into the broad, integrated child protection agenda. Costa Rica offers a particularly good example of how legislative initiatives and policy can come together to enhance children's online protection (see box 10).

Similarly, it is vital for governments to promote awareness and provide skills to children, parents and caregivers to enable them to seek opportunities and prevent and manage harm associated with ICTs.

In their public policies, governments must strike a balance between children's empowerment and protection while not hampering their online opportunities, or their learning to cope with risks.

Data and research are also essential. Sound evidence on children's safety and exposure to online risks is needed to inform law, policy and actions. It is crucial to gain deeper understanding of children's evolving skills, practices and concerns, and their surrounding environment. Knowledge gaps need to be addressed. Studies have often focused more on short-term problems and concerns and less on online opportunities and the long-term consequences of risks. Moreover, few studies have been conducted in countries in the South, or on how very young children engage with ICTs. These are areas where change has been fastest and where the need to minimize risks is particularly important and urgent.

Box 10.
Legal and policy initiatives to promote online protection for children in Costa Rica

In Costa Rica, where as many as 52 per cent of children and young people under 18 were found to own a computer in 2011, decisive legal and policy steps have been taken to enhance children's online protection. Costa Rican legislation criminalizes the production, possession, and distribution of child pornography, whether or not a computer is involved.

In December 2010, a National Commission on Online Safety was established with a multidisciplinary, intersectoral structure and comprising representatives of both public and private institutions. Its role is to devise policies on the safe use of the Internet and ICTs and to develop the National Plan of Online Safety. Specifically, the Commission:

- Raises awareness for children, teenagers and their families about the appropriate use of the Internet and digital technologies;
- Proposes actions to prevent access to inappropriate contents by children;
- Promotes safe access to the Internet and digital technologies;
- Develops strategies to avoid inappropriate use of the Internet or digital technologies in public and private institutions;
- Proposes legislation to strengthen the rights of individuals, communities and institutions regarding access to the Internet.

In light of the rapid evolution of ICTs and the online environment, governments must ensure that appropriate capacity-building initiatives are provided for professionals working with and for children. Too often, professionals lack the training

[232] Ibid., p. 25.

to identify early signals of abuse or address incidents of violence in an ethical, gender-sensitive and child-sensitive manner. They often lack guidance on whether and how they should report such cases. The joint 2011 report of the Special Rapporteur on the sale of children, child prostitution and child pornography and the SRSG on Violence against Children on effective and child-sensitive counselling, complaint and reporting mechanisms recommend that all States consider requiring professionals who work with children to report violence.[233] Clear protocols should be set out to guide professionals as to when and how such reports should be made.

Some professional groups are particularly important actors in this process. These include teachers and social workers, police officials, judges and prosecutors, whose role is crucial both to enhance investigative techniques associated with ICT and Internet-related crime and to ensure that these actors are in the best position to protect and respect the rights of children affected by online criminal abuse.

Effective policing is essential both to prevent violence and abuse associated with ICTs and the Internet and to respond to it. Law enforcement online is particularly challenging given that physical contact need not occur in order for a crime to be committed. Also, much of the evidence involved in these cases is in a volatile electronic format that may elude traditional policing methods.[234] Police investigations in many countries are hampered by a lack of capacity to conduct undercover operations, which are vital in investigating crimes such as grooming and the production and distribution of child sexual abuse materials.

These factors also present challenges to judges and prosecutors, who require specialized training to handle digital evidence and assess the weight and value of this type of evidence, as well as to understand child abuse and exploitation cases associated with the use of new technologies.[235] Investigations are often further complicated by the international dimension of much cybercrime, which calls for cooperation among national law enforcement authorities.

Police forces are also beginning to recognize the importance of an online presence, not simply to detect and prevent crime, but also to interact with and provide advice to children in the online environment. An example is the Facebook page maintained by the Helsinki police. In 2011, 15 to 20 per cent of Internet-related child sexual abuse cases in Finland were reported through the Helsinki Police Department's Virtual Community Policing Group.[236]

Child victims are particularly vulnerable and require appropriate support to avoid the risk of revictimization and to benefit from effective recovery and reintegration.[237] This calls for coordination among the police, the justice sector, social services, education authorities and other relevant entities. In the United Kingdom, CEOP recommends integrating a child protection specialist into police investigations to ensure adequate safeguarding of children and young people.[238] To deal with these challenges, ICMEC, with support from INTERPOL and Microsoft, offers international training programmes to law enforcement officers, prosecutors and other professionals on investigating trafficking and Internet-based crimes against chil-

[233] Joint report of the Special Rapporteur on the sale of children, child prostitution and child pornography and the Special Representative of the Secretary-General on violence against children, 7 March 2011. A/HRC/16/56, §112(a). The report notes that some legislation can lead to an increase in the number of cases reported that, after investigation, are found to be unsubstantiated. See §52.

[234] UN Office on Drugs and Crime, *Comprehensive Study on Cybercrime*, United Nations, 2013, p. xi.

[235] UN Commission on Crime Prevention and Criminal Justice, 'Prevention, protection and international cooperation against the use of new information technologies to abuse and/or exploit children. Report of the Secretary-General', E/CN.15/2014/7, 5 March 2014, §52 & 58.

[236] Forss, Marko, Virtual Community Policing Group, Helsinki Police Department, Finland. Presentation to the expert consultation on 'ICTs and Violence against Children: Minimizing risks and releasing potential', organized by the Office of the SRSG on Violence against Children, Costa Rica, 9-10 June 2014.

[237] Communication from Verónica Donoso, Catholic University of Leuven, Belgium, and EU Kids Online researcher, June 2014.

[238] UNICEF, *Child Safety Online. Global challenges and strategies*, UNICEF, 2011, p. 14.

dren. ICMEC also contributes expertise and outreach capabilities to projects working to enhance operational technology for law enforcement.[239]

Similarly, governments should establish accessible, safe and child-friendly reporting systems and institutions, which should be supported by effective and well-resourced services, and respectful of children's rights.

In this regard, research by EU Kids Online suggests that reporting tools offer a particular benefit to girls, more vulnerable children and children from poorer homes, who often lack alternative resources. The findings also suggest that the more widely and deeply children use the Internet, the more likely they are to use reporting tools if upset by something they encounter online. This being the case, children less experienced in Internet use should be specifically encouraged and enabled to use online tools, and such tools should be easy and simple, to facilitate access by inexperienced Internet users.[240]

Given the enormous social and economic significance of ICTs and the Internet, governments must also take steps to make Internet access widely available to all, including children and young people. This is a requirement for promotion of children's rights to information, participation and freedom of expression—but it also makes sound economic sense for governments to invest in the online literacy of their youngest people. RedNATIC reports that the majority of Latin American countries have implemented policies to provide netbooks for use by school children.[241] In Mauritius, the National Computer Board launched an initiative in 2000 to make information technology facilities available to all communities and to offer special training for women. As of June 2014, its three 'Cyber Caravans' have allowed 156,000 people of all ages to follow ICT literacy and ICT awareness courses.[242]

Raising awareness of the potential risks associated with ICTs and the Internet and how to avoid them is an essential corollary to the rapidly growing use of these technologies. Government public awareness campaigns with safety messages must be developed according to the evolving capacities of specific age groups and the risks they are most likely to encounter. All initiatives of this kind must provide children, parents and caregivers with information on what to do and who to approach should they be concerned for their own safety or that of others.

In cases where a child is harmed, governments must have in place effective services to ensure the child's full recovery and reintegration. In some cases civil society organizations provide such facilities and support, but this does not derogate from the government's responsibility in this respect under article 39 of the CRC.

In addition to applying appropriate legal sanctions against perpetrators of child abuse, it is important that governments take steps, by means of probation services and other appropriate structures, to ensure rehabilitation, after-care and supervision for convicted sex offenders who have returned to society. This is with a view to preventing re-offending and thus to protecting children.

Finally, given our evolving knowledge of how children use the Internet and ICTs, and the rapidly changing online landscape, governments also have an important role in promoting the consolidation of data systems and research. The ITU Child Online Protection initiative provides a significant statistical framework for measuring child online protection, with an emphasis on measures that are suitable for international comparison. The indicators proposed under this initiative are intended to enable Member States to assess the status of child online safety in their country, and identify aspects of child online protection that may require further strengthening.[243]

[239] International Centre for Missing and Exploited Children, 'Pioneering Global Campaigns', ICMEC, n.d., p. 4.

[240] Ibid.

[241] RedNATIC, 'Estado de situación sobre el derecho de la niñez y la adolescencia al uso seguro y responsable de las TIC en 10 países de América Latina', draft version, p. 43.

[242] National Computer Board of Mauritius, 'Cyber Caravan', retrieved 2 June 2014 from <www.ncb.mu/English/EPowering-People/Caravan/Pages/default.aspx>.

[243] ITU, *Child Online Protection. Statistical framework and indicators*, ITU, 2010.

7. Conclusions

The challenge of creating a safe online environment for children lies in developing a range of responses that strike the appropriate balance between maximizing the potential of ICTs to promote and protect children's rights while minimizing the risk and ensuring children's safety and protection.

Children's natural curiosity and sense of adventure must be cultivated and should not be curtailed for fear of encountering risks online. Rather, efforts must focus on developing and implementing child-sensitive and age-appropriate responses that recognize the evolving capacity of children and offer the appropriate degree of freedom and protection for their developmental stage. All children have the right to the skills, knowledge, tools and support to navigate safely online and address issues of concern appropriately, when and if they are encountered. Indeed, all children should be encouraged to capitalize on the full potential of new technologies, not only as users, but also as innovators and creators of content.

The ambition to empower children in the online environment in no way detracts from the responsibility of States to fulfil their legal obligations in this area, including to prevent and respond to all forms of violence against children, and to provide an appropriate framework for self-regulation among corporate sector actors.

This report emphasizes the central importance of promoting a multifaceted agenda and capitalizing on the potential of a wide range of strategic partnerships to promote and safeguard children's rights and address the risks posed to children and young people by new technologies. Essential allies in this process include parents and caregivers, teachers and other professionals working for or with children, as well as civil society partners. Given the commercial nature of the hardware, services, and much of the content of the Internet, the corporate sector is another crucial actor. In line with national legislation and policies, its contribution is significant, including in advocating for and supporting the safeguarding of the rights of the child, providing technical support to police authorities, sharing software and other technology to assist in identifying online risks or tracking perpetrators, and ensuring that appropriate safeguards are integrated into their own software, devices and services.

Achieving the right balance between online protections and opportunities for children and young people requires sound and reliable data. However, as this report emphasizes, ICTs and the Internet represent a rapidly evolving environment about which we still know relatively little.

Significant research gaps exist regarding, for example, the online behaviour of both children and perpetrators of abuse in low- and middle-income countries. Yet solutions need to be adjusted and tailored to countries' different trends in access devices and locations and in usage patterns, attitudes and skill levels.

The growing use of the Internet and ICTs by young and very young children is another key area for research. Little is known about how this group operates online, or about the specific benefits and risks the youngest children encounter. Research is also needed on the specific impact of new ICTs and on previously unknown forms of abuse that have emerged as a result of increased connectivity, such as streaming video of the abuse of children. High-priority areas in this respect include the impact of continued exposure to harmful material and the nature and effect of youth-on-youth exploitation offences.[244]

Similarly, more work is required to help understand the agency of children in protecting them-

[244] UN Commission on Crime Prevention and Criminal Justice, 'Prevention, protection and international cooperation against the use of new information technologies to abuse and/or exploit children. Report of the Secretary-General', E/CN.15/2014/7, 5 March 2014, §44.

selves and others from online threats; how the role of children and young people varies from one national or regional context to another; and how socioeconomic, political, cultural and geographical factors influence their online behaviour. Other areas needing attention are children's involvement in cybercrime, including hacking and scamming, cyberbullying and harassment, and the consumption, production and dissemination of child sexual abuse material. Responses should focus on restorative processes and avoid criminalizing children.

The engagement of the corporate sector and civil society in initiatives to protect the rights of children online and prevent and respond to child abuse does not derogate from States' responsibility to protect the rights of the child. Indeed, the role of national authorities is crucial in ratifying and implementing relevant international standards; establishing a clear and comprehensive legal and policy structure to ensure explicit prohibition of all forms of violence against children, including in cyber space, and effective protection of child victims; coordinating and assessing the effectiveness of the implementation of these initiatives; ensuring that structures are in place to train professionals; supporting parents and caregivers to develop their own digital skills; and setting out responses to illegal online activity, both in terms of support, recovery and reintegration for victims and penalties and rehabilitation for offenders.

The role of the State is equally essential in creating a protective online environment for children, in which they can develop their digital skills without fear. In addition, governments must take steps to ensure access to technology for all children and young people. This measure is consistent with the right of the child to information while addressing the risk of some children being left behind as technology advances. It also represents a sound economic investment in the future.

While data are still lacking and many findings are inconclusive, one of the consistent themes to emerge from research is the gap between the experience and perception of parents and caregivers of ICTs on the one hand, and children and young people on the other. With time this generational gap is likely to narrow, but for now this trend limits the ability of parents and caregivers to provide children with much-needed guidance and protection. In this environment, the role of schools is particularly significant in enhancing children's knowledge and skills, offering support and, where appropriate, encouraging digital literacy among parents and in the community.

The benefits of technology and its potential to empower children, together with recognition of the resourcefulness and evolving capacity of children to take an active role in their own protection and that of others, must lie at the heart of all initiatives. The Convention on the Rights of the Child was developed at a time when the full impact of the Internet and ICTs on our lives could scarcely be imagined. Yet, in unambiguously setting out the rights of the child "to seek, receive and impart information and ideas of all kinds, regardless of frontiers" and to benefit from "appropriate legislative, administrative, social and educational measures to protect the child from all forms of physical or mental violence, injury or abuse, neglect or negligent treatment, maltreatment or exploitation," the Convention lays the very foundation for the pressing task we must address.

7.1. Crucial steps for a safe, inclusive and empowering digital agenda for children

1. Governments should ratify and effectively implement all relevant international child rights instruments, including the Convention on the Rights of the Child and its Optional Protocols on the sale of children, child prostitution and child pornography, and on a communications procedure. They should also pursue international cooperation to safeguard children's right to freedom from violence.

2. Empowering all children, wherever they live, is critical to tap into their resourcefulness and enhance their resilience while exploring the potential of ICTs. Children's views should be given due consideration in this process. Guided by ethical standards, children should be involved in research and development of advocacy and policy action to capitalize on the potential of ICTs and the Internet and to minimize and respond to risks associated with them.

3. Governments should pass comprehensive legislation to ban all forms of violence against children, supported by specific legislation relating to the online risks that children may encounter. Whenever possible, this legislation should be 'technology neutral', so that its applicability is not eroded by future technical developments. All relevant actors should be aware of this legislation and support its effective enforcement.

4. Effective, well-resourced and coherent national policies to prevent and address violence against children including online abuse are essential and must incorporate clear time-bound goals and responsibilities. These policies should support families in their crucial role, capitalize on the potential of schools, build upon strategic partnerships with civil society and the corporate sector, and explicitly recognize and address the situation of particularly vulnerable children. An effective monitoring and evaluation system should be put in place to assess the impact of these policies.

5. All professionals working with and for children should have the knowledge to address the risks children face online, to recognize the signals that suggest a child may be a victim of online harm and the skills to take appropriate steps in response. Professionals working in related fields should be mandated to report online violence and abuse against children.

6. Safe and easily accessible child-sensitive counselling, reporting and complaint mechanisms, such as helplines, should be established by law and constitute core dimensions of the national child protection system, with appropriate links to child support services and law enforcement. Telecommunications companies should consider waiving costs for incoming calls to child helplines by means of toll-free numbers.

7. Children who are victims of violence, abuse or exploitation should benefit from effective remedies and appropriate, adequately resourced recovery and reintegration services. These should be supported by well-trained child protection specialists

OFFICE OF THE SPECIAL REPRESENTATIVE OF THE SECRETARY-GENERAL ON

VIOLENCE AGAINST CHILDREN

The Special Representative of the Secretary-General on Violence against Children is an independent global advocate in favour of the prevention and elimination of all forms of violence against children, mobilizing action and political support to achieve progress the world over. The mandate of SRSG is anchored in the Convention on the Rights of the Child and other international human rights instruments and framed by the UN Study on Violence against Children.

www.violenceagainstchildren.un.org