Comment to the Committee on Rights of the Child on children's rights in digital environments

Date: May 15, 2019
Organization: Global Partnership to End Violence Against Children
Contact person: Trang Ho Morton, Fund Partnerships
Contact details: trang.ho.morton@end-violence.org

Information about the organization: Since its inception in 2016, the Global Partnership to End Violence Against Children and its associated Fund (End Violence) has invested close to $32 million in 37 projects across 27 countries to combat violence against children and adolescents, primarily in digital environments. Projects supported by End Violence provide a range of services, including: (i) rescuing victims and supporting survivors; (ii) raising awareness of the problem and contributing to behavioural change; (iii) strengthening law enforcement and legislative reforms; and, (iv) developing solutions within the technology and online service provider community. In March 2019, End Violence announced a large-scale research project - *Disrupting harm: evidence to understand online child sexual exploitation and abuse* – designed to collect evidence in 14 countries on child sexual exploitation and abuse and other crimes against children in digital spaces.[1] Later this year, End Violence will focus investments on the development and roll-out of digital technologies to strengthen prevention and response systems against the most prominent forms of violence against children in digital environments. Special attention will be given to enhancing national capacity and infrastructure to ensure cross-sector collaboration and the engagement of industry players to support the adoption of technology solutions.

Focus of the comment: End Violence recognizes that the rights of children as enshrined in the Convention on the Rights of the Child (CRC) and its Optional Protocols carry equal value and importance for children, for adults with a responsibility to protect children, and for society in its entirety. Violence against children, whether direct or indirect, affects children's ability to enjoy their rights. End Violence also recognizes that the diverse forms and reach of violence against children is increasing in digital environments, impacting upon the many positive and therefore protective opportunities that the digital environment may offer. Evidence generated under End Violence's efforts demonstrates an urgent need to recognise the vast and pervasive impact of digital technologies on children's ability to exercise their full rights. We recommend that the potential for both positive and negative impact of the digital environment is reflected in the CRC and Optional Protocols. The recognition that violence against children is prevalent in nearly all dimensions of children's lives - both online and offline - ensures the full and fair protection of all human rights.

1. Context

Every day, nearly 200,000 children worldwide are initiated onto the online environment. Joining millions of others, these children benefit from evolutions in digital technology that are enabling new levels of creativity and innovation, enriching the very educational and life opportunities that the CRC laid out 30 years ago.

However, these largely positive effects of technological development are increasingly accompanied by unintended risks and harm for its users, both children and adults, and in most cases the risks go undetected until children have already been exploited. Digital environments provide those seeking to harm children with unprecedented levels of access, new capabilities and increasing confidence to do harm on a mass scale.

In an era where the divide between 'online' and 'offline' violence is increasingly understood to be artificial, the impact of harm committed against children in digital environments can be as severe as similar harms committed

[1] **Africa**: Ethiopia, Kenya, Mozambique, Namibia, Rwanda, South Africa, Tanzania, Uganda. **Southeast Asia**: Cambodia, Indonesia, Malaysia, Philippines, Thailand, Vietnam. Implemented collaboratively by Interpol, UNICEF Innocenti and ECPAT, the project will pilot an innovative new methodology to determine the context, scale and manifestations of these crimes. It combines primary and secondary data collection, including contextual research, offence-related data and surveys with children using the Global Kids Online methodology. The framework and outputs are envisioned as an important step towards data collection and in-depth analysis of online crimes against children. Findings are expected in the first quarter of 2021.

offline, and often have long-lasting consequences that limit the capacity of child victims and survivors to live a full life.

2. Key risks and threats for children and adolescents

Indeed, in the first Global Threat Assessment of its kind on online child sexual exploitation and abuse (CSEA) in 2018, the WeProtect Global Alliance (WPGA)[2] described online CSEA as the "most insidious form of modern cybercrime." It describes the most prominent manifestations of online CSEA to include production and distribution of child sexual abuse material (CSAM), live streaming of child sexual abuse, online sexual grooming and sextortion, and increasingly the production of "self-generated CSAM".[3]

In recent years, the volumes of CSAM have increased exponentially and in unprecedented ways, marked by a rapid increase in the volume of videos over images, and facilitated by rapid increases in Internet penetration and the decreasing costs of connectivity, software and hardware including smartphones and storage devices. The statistics are alarming: over a six-week period in 2017, the newly developed automated website crawler (Project Arachnid) managed by the Canadian Centre for Child Protection, processed over 230 million web pages and detected over 5.1 million unique web pages hosting 40,000 unique images of child sexual abuse.[4] According to EUROPOL, in 2018, 60% of EU Member States reported an increase in the online distribution of CSAM.[5] Finally, the number of CyberTipline reports received by NCMEC (National Center for Missing and Exploited Children) grew nearly tenfold in 3 years, from 1.1 million in 2014 to 10.2 million by 2017, and almost doubled in 2018 with 18.4 million reports received. The violation of children's rights online is both a grave and growing problem that requires urgent attention.

The rapid spread of the Internet has also enabled the proliferation of online communities of child abusers, including darknet sites that exist across the full spectrum of CSAM offences. One such service, for instance, has over 18,000 registered members and is described as dedicated to infant/toddler abuse. Many have registered members in the tens or hundreds of thousands. The US Department of Justice reports that an aggregate 1.9 million users are registered across nine sites dedicated to this material.[6] While CSAM remains accessible and is shared on the open web, including via social networks, networked environments such as peer-to-peer (P2P) and anonymized Darknet networks (e.g. Tor) remain the main platforms used to access CSAM and the principal means for non-commercial distribution[7]. Other environments such as encrypted mobile apps and services, gaming platforms, cloud storage, encryption and anonymizing technologies including cryptocurrency and frontier technologies are also facilitating the proliferation and storage of online CSAM targeting children for other forms of online CSEA. For instance, offenders use chat rooms to promote and share content, including discussions on how to bypass law enforcement.

3. Key gaps, challenges and underdeveloped areas

Since the adoption of the CRC in 1989 and the Optional Protocol on the sale of children, child prostitution and child pornography in 2000, violence against children in digital environments has transitioned from being a new form of violence to a pervasive phenomenon impacting children in every dimension of their lives including in their homes, communities and schools. It is also an increasingly complex, voluminous and evolving form of violence that is at the same time distinct from and yet inextricably interwoven with violence, abuse and exploitation in the 'offline' world, presenting significant challenges for both prevention and response.

Key gaps, challenges and underdeveloped areas of attention include:

- Existing legislative and regulatory frameworks that govern the use and application of digital technologies and platforms, as well as investigation and prosecution of crimes committed through them, are often

[2] www.weprotect.org/.

[3] Self-generated, or youth-produced CSAM, initially shared with innocent intent, often finds its way to "collectors", who often proceed to exploit the victims, in particular by means of extortion (EUROPOL, IOCTA, 2018). It is worth noting that in most cases self-generated CSAM is illegal, but the act depicted is often not illegal. However, the self-generated CSAM needs to be detected, reviewed and removed like all other CSAM.

[4] https://www.cybertip.ca/app/en/projects-arachnid, 2017.

[5] EUROPOL, Internet Organised Crime Threat Assessment (IOCTA), 2018.

[6] Quoted in WeProtect GTA 2018, from US Department of Justice, January 2018.

[7] EUROPOL, Internet Organized Crime Threat Assessment (IOCTA), 2018.

outdated, too conventional or insufficiently agile to keep up with the fast-emerging manifestations of the problem.

- Perpetrators are benefitting from advanced technology, too often requiring law enforcement and industry to catch up in their response. The unprecedented speed and ease of producing and sharing content, expanded access to content and children online, and the ability to go undetected also require a more targeted focus on demand. Indeed, despite promising programmes to respond to and help prevent offending against children in some countries, preventive and response services for the offender and potential offender population remain limited or non-existent in most countries. There is a clear and pressing need for sharing of both good evidence-based practice proven to prevent and reduce offending and/or recidivism.
- The open source programming origin, single purpose and/or commercial objective behind many new digital technologies, products and services either mean that sometimes no one individual or company can be held liable for their use or misuse, or that they are often designed with limited or no consideration about the ways these could be used to exploit or abuse a child.
- In digital spaces, the fact that 'users are also producers' of digital content and products brings additional challenges to the regulation of digital technologies and environments. Responsible technology and ethics by design require a shift in mindset and awareness, and potentially a shift in legislative and regulatory ecosystems, including but not only in relation to online CSEA but also for other forms of violence against children and their subsequent violation of rights.
- The lack of reliable data, research and a clear understanding of evidence-based solutions that work remains a significant obstacle for program design and advocacy efforts. There is still only a partial understanding of the socio-economic, technological, cultural drivers and both risk and protective factors that underpin harmful practices against children in digital environments. Few of the solutions that do exist actually equip children to protect themselves within a largely pervasive Internet environment.
- The general under-resourcing of and limited attention to awareness, knowledge generation and exchange across sectors and actors, including among children, adolescents, caregivers, media and society, continues to hamper the effectiveness of preventive and response systems.
- Limited and uneven country capacity, capability and infrastructure to engage with multiple actors, and particularly the ICT sector and tech industry, limits progress. Regional investment disparities persist, and there remains limited expertise in most countries in the South, and limited opportunities for South-South learning on the topic.

4. Progress to date and way forward

Despite significant progress in the realms of technology, data and evidence generation and awareness and knowledge exchange worldwide, much remains to be done. Key areas of focus include:

- Low-cost, scalable and platform-agnostic technological solutions to respond to these challenges at the international level. Significant advancements have been made in technology and capacity worldwide to tools respond to online CSEA, with much focus to date being on CSAM[8]. However, as the volume of content continues to grow, the technology must keep pace by continuing to assist humans with automated processes that increase efficiencies and free up precious time for the investigation of new and urgent cases. And the technological and social challenges presented by the live streaming of CSEA, online grooming of children and youth-produced sexual content need a more advanced and coordinated response[9].

[8] For instance, groundbreaking technology is helping detect and remove CSAM from online platforms. By July 2018, the ICSE Database (International Child Sexual Exploitation) managed by Interpol helped to identify 14,200 child victims and 6,200 offenders around the world and reduce duplication of investigation by law enforcement. Technology such as PhotoDNA (developed by Microsoft and Dartmouth College in 2009) is now used by numerous organizations to detect, report and remove millions of images.

[9] In recent years for example, there has been an increasing number of reports related to online grooming of children for sexual purposes, as a clear channel for perpetrators to coerce or extort the child into producing sexualized images or engaging in sexual activities via webcams[99]. Data on online grooming from the UK suggest that children are most frequently lured or manipulated into self-produce sexual images or videos without any intention by the "groomer" of meeting the children in real life. In the 18 months since sexual communication became an offence in the UK (April 2017) the police recorded more than 5,000 online grooming offences.[9] International standards do not yet fully reflect this new phenomenon; therefore, prevention remains essential and technological solutions could possibly play a critical role.[9]

- A stronger and broader evidence base in all countries and regions to gain insight into the scale and nature of the problem, recognizing the importance of national participation in the process of discovery, is essential to inform the design of effective prevention and response strategies.
- Increased attention to prevention of offending and victimization of children as the best approach to achieve sustainable results at scale and ultimately ensure that children are safe in digital environments.
- Enhanced cross-sector collaboration and engagement modalities, particularly with and across industry players, are needed. Industry (broadband, Internet providers, regulators, operators, tech community, etc.) remains a vital stakeholder to tackle this problem, both because it develops and provides many of the services that are being misused, but also because of its potential to exploit its power to drive technological policy and practice. Larger companies and tech giants have undoubtedly invested in this area, but more could still be done to create new ethical standards that ensure their platforms are free of harmful activities against children, and that smaller companies can benefit from and be encouraged to adopt scalable strategies to address the issue on their own platforms and services.
- Addressing the legal, data protection, language and socio-cultural obstacles to cooperation across sectors and between countries. This will require a political and cultural shift and change from single sector investments to multi-sectoral working modalities.

To conclude, digital environments are now integrated into every aspect of our lives, and this is as true for children as it is for adults. Worldwide, the opportunities these environments offer for the fulfilment of children's rights are immense and unprecedented. Building upon these protective solutions and responses is a moral obligation supported under the CRC. However, the many positive opportunities are also accompanied by serious risks to children's safety. These risks and harms are expanding and diversifying as fast as technology develops, leading to devastating consequences for children that transcend the now largely artificial boundaries between 'online' and 'offline'. Identifying these harmful practices, and their pathways, is a priority in order to identify the most effective interventions to prevent violence in the first place.

While significant progress has been seen in responses by governments, industry, civil society and other actors to address and counter the unintended consequences of the digital era for children, it is time to bring the digital environment into a new and central focus to ensure the furtherance and protection of children's rights all over the world. In conclusion, End Violence hereby recommends that the digital environment be amply reflected as such in the CRC and Optional Protocols.

Annex 1: Key documents and publications

- UK Home Office, Online Harms White Paper (UK only), 2019
- PA Consulting, A tangled web: rethinking the approach to online CSEA, 2019
- UK Information Commissioner Office, Consultation on Code of Practice to help protect children online (UK only), 2019
- Global Fund to End Violence against Children, Disrupting Harm: evidence to understand online child sexual exploitation and abuse, 2019
- Global Partnership to End Violence against Children, Safe to Learn Call for Action, Youth Manifesto, 2019
- UNESCO, Behind the numbers: Ending school violence and bullying, 2019 (includes data on online hurtful behaviour and cyber-bullying)
- WeProtect Global Alliance, Global Threat Assessment, 2018
- Child Dignity on the Digital World, Technical Working Group Report, 2018
- Global Fund to End Violence against Children, Two years of supporting solutions: results from the Fund's investments, 2018
- WeProtect Global Alliance, Country examples of Model of National Response capabilities and implementation, 2018
- INTERPOL and ECPAT International, Towards a Global Indicator on Unidentified Victims in Child Sexual Exploitation Material, 2018
- EUROPOL, Internet Organised Crime Threat Assessment (IOCTA), 2018
- NetClean, Report about Child Sexual Abuse Cybercrime, 2018
- ICMEC, Sexual Extortion and Non-consensual Pornography, 2018
- International Association of Internet Hotlines, INHOPE Report, 2018
- Thorn, Production and Active Trading of Child Sexual Exploitation Images , 2018
- ITU, Global Cybersecurity Index, 2018
- USA Dep of State, Trafficking in persons report, 2018
- CSA Centre of Expertise, Interventions for perpetrators of online child sexual exploitation - a scoping review and gap analysis, 2018
- NatCen, Behaviour and Characteristics of Perpetrators of Online-facilitated CSEA - a rapid evidence assessment, 2018
- NCMEC, The online enticement of children: an in-depth analysis of CyberTipline Reports, 2017
- 5Rights Foundation, Digital Childhood, childhood development milestones in digital environment, 2017
- Internet Watch Foundation (IWF), Annual Report, 2017
- ICMEC, Annual Report, 2017
- Thorn, Sextortion online survey with 2,097 victims of sextortion ages 13 to 25, 2017
- UNICEF, Children in a Digital World, 2017
- ECPAT International, Sexual Exploitation of Children in South East Asia, 2017
- UNICEF, Perils and possibilities: growing up online, 2016
- UNICEF, Child protection in the digital age: National responses to online CSEA in ASEAN, 2016
- Centre for Justice and Crime Prevention, Child Online Protection in the MENA Region, 2016
- Luxemburg Terminology Guidelines for the Protection of CSEA, 2016
- WeProtect Model of National Response, 2015
- NCMEC, A Global Landscape of Hotlines Combating CSAM, 2015
- ITU and UNICEF, Guidelines for Industry on Child Online Protection, 2015

Other resources:

- Global Resource and Information Directory (GRID) challenges and responses to child online safety
- ITU Child Online Protection Country Profiles Case Studies
- Child Online Safety Industry good practice and country examples
- Child Online Protection Tools for ICT companies
- Council of Europe, Children and the Internet resources
- Think you know, Resources for children, parents and professionals
- Australia eSafety Commissioner, Child online safety resources
- Canadian Centre for Child Protection, Online safety resources for children and parents
- Power of Zero, Global campaign to reshape early learning for a connected world
- EU Kids Online
- Global Kids Online