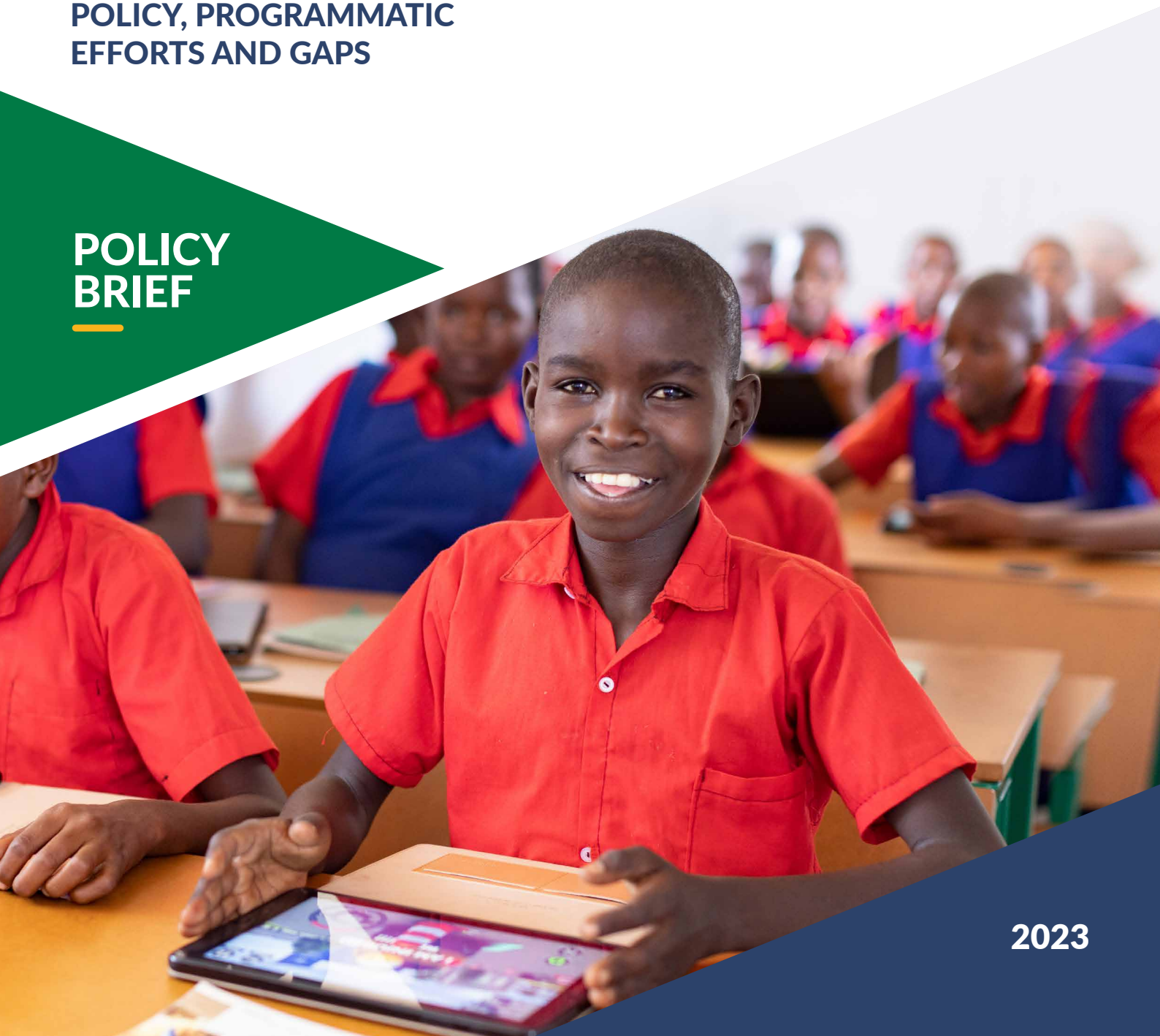
ChildFund®
Because we need each other.

African Child Policy Forum
ACPF

Online Child Sexual Exploitation and Abuse (OCSEA)

POLICY, PROGRAMMATIC EFFORTS AND GAPS

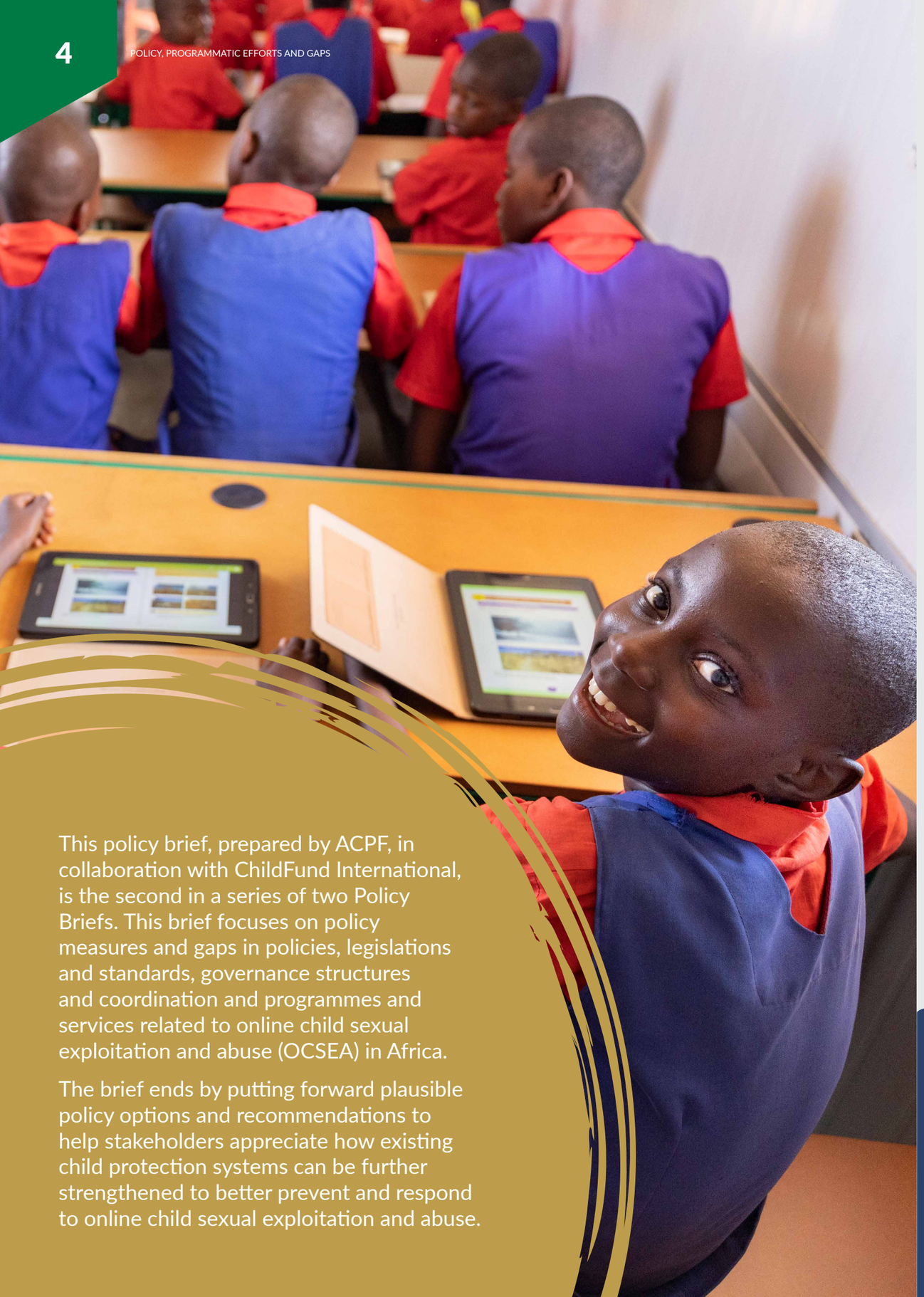
POLICY BRIEF



2023

The internet has offered countless opportunities for children for learning, for networking and for recreation, among others. But it has also presented challenges that are very subtle, fast-evolving and hard to contain. One such challenge that African governments and other stakeholders are struggling with is the online sexual abuse and exploitation of children.

Contents



This policy brief, prepared by ACPF, in collaboration with ChildFund International, is the second in a series of two Policy Briefs. This brief focuses on policy measures and gaps in policies, legislations and standards, governance structures and coordination and programmes and services related to online child sexual exploitation and abuse (OCSEA) in Africa.

The brief ends by putting forward plausible policy options and recommendations to help stakeholders appreciate how existing child protection systems can be further strengthened to better prevent and respond to online child sexual exploitation and abuse.

1. Efforts to address online child sexual exploitation and abuse

Many African countries are working towards improving access to the internet for all, especially children in schools and elsewhere. For example, Namibia, in 2020, introduced a National Broadband Policy which also involved children in the development process, and commits to provide broadband internet in all schools by 2030. And yet, internet access in Africa is also hampered by internet blockages. In 2022 alone, seven countries in Africa were recorded to have shut down the internet nine times.[1] Limited access to the internet infringes children's rights, among others, to education, freedom of expression, freedom of association and the right to play.[2]

The internet has offered countless opportunities for children for learning, for networking and for recreation, among others. But it has also presented challenges that are very subtle, fast-evolving and hard to contain. One such challenge that African governments and other stakeholders are struggling with relates to online child sexual abuse and exploitation. This is a crime that has a global grip and with a very high level of complexity. In addition to the dearth of strong research evidence on the issue, the legislative and policy landscape in Africa has lagged far behind the fast pace of sophistication and cutting edge modus operandi of crimes in cyber space. A research undertaken by the African Union (AU) in preparation for the development of its strategy and plan of action on OCSEA indicates that none of the 55 African countries have all the six key capabilities identified (in the Model National Response, developed by the WE Protect Global Alliance) as key to preventing and responding to OCSEA: policy and governance, criminal justice, victim, societal, industry and media and communications capabilities.[3]

African governments, despite being relatively late comers in terms of appreciating the scale and impact of the problem, are increasingly acknowledging the dangers of the digital world and exploring ways to address online child sexual exploitation and abuse (OCSEA).

Different policy measures have been designed and implemented with the aim of strengthening existing child protection systems and better protect children online. Yet, progress is still hampered by limited evidence and understanding of OCSEA, lack of effective regulations as well as limited technological capabilities. As technology is used to facilitate online child sexual abuse and exploitation, tech companies also bear a special responsibility especially through the prevention of exposure of children to sexual images and videos. Non-governmental organisations, on the other hand, are also playing important roles in case referrals, victims support, awareness raising, and training frontline service providers; however, their engagement in research, policy advocacy and development of appropriate tech solutions remains limited.

In the section below, we examine the various measures taken by governments, non-governmental organisations and the private sector (particularly the tech industry) to strengthen national child protection systems to be able to effectively respond to online child sexual exploitation and abuse (OCSEA).

Limited access to the internet infringes children's rights, among others, to education, freedom of expression, freedom of association and the right to play.

1.1: The Model National Response to OCSEA

The Model National Response (MNR) is the most commonly used approach/framework to review countries preparedness to effectively prevent and respond to online child sexual abuse and exploitation. The MNR considers 21 capabilities (categorized under seven capabilities) that a country needs in order to achieve a comprehensive national response in the context of the wider needs to tackle all forms of sexual abuse and exploitation of children. The MNR is aligned with the child protection system approach which looks into legal and policy frameworks, governance and coordination structures, programmes and services, resources (human and financial) as well as monitoring and oversight that are all needed to prevent and respond to risks associated with online child sexual abuse and exploitation.[1]

1.1 Legal and Policy Frameworks

There are a number of global and regional instruments that provide protection for children from online sexual abuse and exploitation. The United Nations Convention on the Rights of the Child (CRC), under article 34 and 36 require States to protect children from all forms of sexual exploitation and sexual abuse. The Committee on the Rights of the Child also adopted a General Comment 25 on Children's Rights in Relation to the Digital Environment, which acknowledges the importance of child rights in the digital environment and places obligations on states and businesses to take the necessary action.[4]

At Pan-African level, Africa's Agenda for Children 2040, under aspiration 7, stipulates that no form of violence against a child (which also includes OCSEA) is justifiable and that children have a right to be protected from violence.[5] Besides, the African Charter on the Rights and Welfare of the Child (ACRWC), under Article 27, requires States Parties to protect children from all forms of sexual exploitation and sexual abuse. The Charter obliges State Parties to take measures to prevent the inducement, coercion or encouragement of a child to engage in any sexual activity, the use of children in prostitution or other sexual practices including "pornographic" activities, performances and materials.

The AU Commission has done its part in terms of supporting the creation of a harmonised regulatory framework for ICT development. Notable among these efforts include the adoption of the AU Convention on Cyber-security and Personal Data Protection, the Continental Cybersecurity Strategy, the Continental Child Online Safety and Empowerment Policy, and AU's Strategy and Plan of Action on Strengthening Regional and National Capacity and Action against Online Child Sexual Exploitation and Abuse in Africa (2020 – 2025). The AU Convention on Cybersecurity and Personal Data Protection (2014), known as the "Malabo Convention", is coming into force after Mauritania recently became the 15th state to submit its ratification in May 2023.[6] The Convention is particularly relevant for criminalising the exploitation of children for sexual activities and performances.

Apart from the Malabo Convention, another important framework that was adopted by the AU is the AU Strategy and Action Plan against Online Child Sexual Exploitation and Abuse (2020 – 2025). The Plan of Action aims to put in place a comprehensive and coordinated effort to accelerate actions by the relevant stakeholders in addressing Online Child Sexual Exploitation and Abuse (OCSEA) including prevention, protection and prosecution.[7] Besides this, the AU has introduced initiatives relevant to addressing OCSEA issues. One of these landmark initiatives was achieved in 2019 when the AU hosted a Global Summit to Tackle Online Child Sexual Exploitation in collaboration with We Protect Global Alliance which brought together over 700 high-level representatives of governments, the private sector/ industry, civil society organizations, regional mechanisms/ entities, and specialized agencies of the United Nations.[8] The Summit, among other things, committed all relevant stakeholders to collaboration, undertaking research and sharing good practices on preventing and tackling OCSEA. The Summit also called on AU Member States to reaffirm the African Union Convention on Cyber Security and Personal Data Protection (the "Malabo Convention") and develop national action plans to tackle online child sexual exploitation.[9]

Another important initiative was a project that was implemented between 2018-2022 by the AU Commission entitled 'Strengthening Regional and National Capacity and Action against Online Child Sexual Exploitation (OCSE) in Africa." The project was critical in identifying gaps and priority areas for the AU's engagement on OCSEA and eventually resulted in the development of AU's 5-year Strategy and Plan of Action (2020 – 2025) on OCSEA.[10] Despite these commendable initiatives, there is a dearth of information if AU's legal and policy frameworks have translated to concrete actions in terms of strengthening the regulatory environment at national level. In 2022, the AU convened a workshop attended by senior government officials from 16 countries in Africa, Interpol, CSO's including World Vision International and ChildFund International, that resulted in the development of a roadmap for tacking OCSEA in the continent.

The African Committee of Experts on the Rights and Welfare of the Child (ACERWC) has also been engaged with the issue over the past few years. The Committee issued a General Comment on Sexual Exploitation which seeks to extend the understanding of the implications of article 27 of the ACRWC to the online environment by addressing online child sexual exploitation.[11]The General Comment, among others, clarifies the additional responsibility/obligation of State Parties to educate and empower families and children on OCSEA and also to adopt clear measures for a safe online environment. Besides, in 2019, the ACERWC conducted a Day of General Discussion on OCSEA during its 33rd ordinary session with the aim of providing guidance to State Parties on how to protect children from online child sexual exploitation through policies, legislation, law enforcement and programmes.[12] The event was particularly critical in that the Committee considered the importance of developing a General Comment on Article 27 of the ACRWC to expand the implications of article 27 to include issues related to OCSEA.[13] Most recently, the ACERWC's Working Group on Children's Rights and Business also resolved (Resolution 17/2022) on the promotion and protection of children's rights in the digital sphere.

30 **African countries have no law or policy on cyber security, not even a draft, as the ACERWC noted in 2021.**

At sub-regional level, the Regional Economic Communities (RECs) have also put in place policy measures for the protection of children in the digital world. The EAC Framework for Cyber laws (2008), for example, is one such effort. The purpose of the law is to promote regional harmonisation in the legal response to the challenges raised by the increasing use and reliance on ICT for commercial and administrative activities, specifically in an Internet or cyberspace environment.[14] The Southern African Development Community (SADC) has also put in place a Model Law on Computer Crime and Cybercrime that criminalises child pornography.[15]

Apart from the EAC and SADC, ECOWAS has also put in place a Directive on Fighting Cyber Crime (2011) which provides for offences related to using children for sexual performances and activities.[16]

At national level, several countries have ratified important international and regional treaties relevant to address online child sexual exploitation and abuse (both online and offline): UN Convention on the Rights of the Child (ratified by all), Optional Protocol to the Convention on the Rights of the Child on the Sale of Children Child Prostitution and Child Pornography (ratified by all except Sahrawi Arab DR, Sao Tome & Principe, and Somalia), the African Charter on the Rights and Welfare of the Child (ratified by all except Morocco, Sahrawi Arab Democratic Republic, Somalia, South Sudan and Tunisia) and the African Youth Charter (ratified by 40 countries).

Notwithstanding the ratification of these important instruments and corresponding efforts to introduce legislation, very few countries have legislative frameworks specifically designed to comprehensively address OCSEA.[17] Most countries have legislation that criminalizes some aspects of online child sexual exploitation and abuse.[18] As the ACERWC noted in 2021, 30 African countries have no law or policy on cyber security, not even a draft.[19] Other than that, in most African countries, legislations fail to either clearly define nor criminalise child sexual abuse material or online grooming with the intent of sexually abusing children. This leaves a loop hole for predators to continue committing crimes against children with impunity. Studies have confirmed that where laws on cybercrimes are inexistent or ineffective, sex offences are likely to proliferate. Interestingly, online sex offenders have been reported to seek or offer information about places or countries in which laws protecting against sexual exploitation - online or offline - may be lax or not enforced.[20] There are instances where offenders engage in chat and in forums where they can elicit information on how to better exploit a lawless space or how-to-avoid-law-enforcement.[21]

The industry (such as the technology, telecommunication, ICT industries) has a special role in the fight against child sexual abuse and exploitation. Strong regulation is required for the tech sector and internet service providers around reporting or taking down procedures of child abuse materials.

Online sex offenders will primarily choose and utilize a perceived lawless space that best meets their psychosocial and criminogenic needs in the most frictionless way; habituation and differential association in the lawless space will reduce the perceived risk; normalization will increase comfort in a particular lawless space, increasing friction costs that must be overcome to switch technologies; and additional countermeasures will only be implemented by offenders to reduce perceived risk and lower cognitive dissonance, but not at the expense of utility (Steel et al. 2023:1).

A major challenge in Africa is that there are no established procedures for blocking or taking down child abuse material from the web.[22] Internet service providers in many African countries are not obliged by the law to retain data, filter/block/take down child sexual abuse materials (CSAM) and comply promptly with law enforcement requests for information.[23] Because of absence of regulations and obligations to report OCSEA materials, countries have a very long way to go in terms of holding internet and telecommunications service providers accountable for violations.[24]

Notwithstanding the challenges, some countries offer good practice examples. Recently, Kenya adopted Children's Act (2022) which defines and criminalises grooming, penalizing criminals to ten years imprisonment for a term not exceeding ten years or to a fine not exceeding two million shillings, or to both.[25] Similarly, Zimbabwe has recently included child-specific provisions in its Cybercrime Bill, thereby aligning the Bill with international standards.[26] South Africa also amended its legislation relating to sexual crimes – the Sexual Offences and Related Matters Amendment Act 32– which seeks to improve coverage of OCSEA issues, such as grooming children within the scope of the law. The legislation now criminalises grooming children with the intent of sexually abusing them, such as the production and display of child sexual abuse material (CSAM) through the internet and other information and communication technologies.[27] The country's Film and Publications Board Act (1996) (as amended) criminalizes the failure to report images or occurrences of child pornography about which one is aware to relevant authorities.

Ghana and Côte d'Ivoire also offer good examples. In 2020, Ghana, through its Ministry of Communications and the National Cyber Security Centre (NCSC), and in collaboration with the Internet Watch Foundation (IWF) launched an online child protection reporting portal to help receive reports of child sexual abuse materials and enable immediate action in terms of taking down these materials from the internet.[28]

Botswana also has some strong laws with regards to child sexual abuse material" (CSAM). Section 16 of the Cybercrime and Computer Related Matters Act 2007[29] of Botswana defines the term "child pornography" to include material that visually or otherwise depicts: (i) a child engaged in sexually explicit conduct; (ii) a person who appears to be a child engaged in sexually explicit conduct; or (iii) realistic images representing a child engaged in sexually explicit conduct.

The Botswana children act of 2009 also prohibits CSAM. Sec. 58 prohibits exposing children to CSAM, making such material available to a child, or involving a child in the making of such material. It also prohibits anyone from storing, keeping or distributing any indecent images of a child depicting any form of illegal sexual activity against a child.[30]

Beyond governments, civil society organisations and international organisations play an important role in the development of guidelines and setting standards. The Model National Response (MNR), developed by the WeProtect Global Alliance, for example, is an important framework which guides countries on the kind of capabilities they need to have and develop in order to better prevent and tackle OCSEA.[31] According to the MNR, countries need to have capabilities in six areas: policy, legislation and governance, criminal justice, victim support, society and culture, industry, and research and data.[32] A research undertaken by the AU indicated that 55 Member States notes that none had achieved the requirements in all the six pillars of the Model National Response (MNR). Kenya, Ghana and South Africa are the only countries that have policies as it relates to tackling OCSEA.

In general, as the ACERWC noted, most laws and policies in Africa tend to focus on the exploitation of children for "pornographic" activities and barely address other forms of online child sexual abuse and exploitation such as online grooming, cyberbullying, and exposure to harmful or inappropriate content, among others. Laws and policies are only as good as their implementation and enforcement. Implementation requires political commitment to put in place structures and systems. In this regard, there remain significant challenges.

1.2 Governance and Coordination Structures

This is about the presence as well as functional clarity of governance and leadership structures at the highest level, multi-sectoral coordination bodies at different levels, their roles and capacities to address child protection issues and concerns. It is also about how various actors- state and non-state actors (NGOs, community based organisations, faith based organisations, businesses, ICT companies), children, families, and the community interact and work together to address existing and emerging child protection issues.

Child protection, especially in the digital environment, spans multiple sectors, including education, health, social services, and also involves multiple types of stakeholders, including the Government, civil society, community based organisations, faith-based organisations, international organisations, academia and the private sector. The unique nature of online child sexual abuse and exploitation also necessitates cross border cooperation amongst countries, particularly law enforcement.

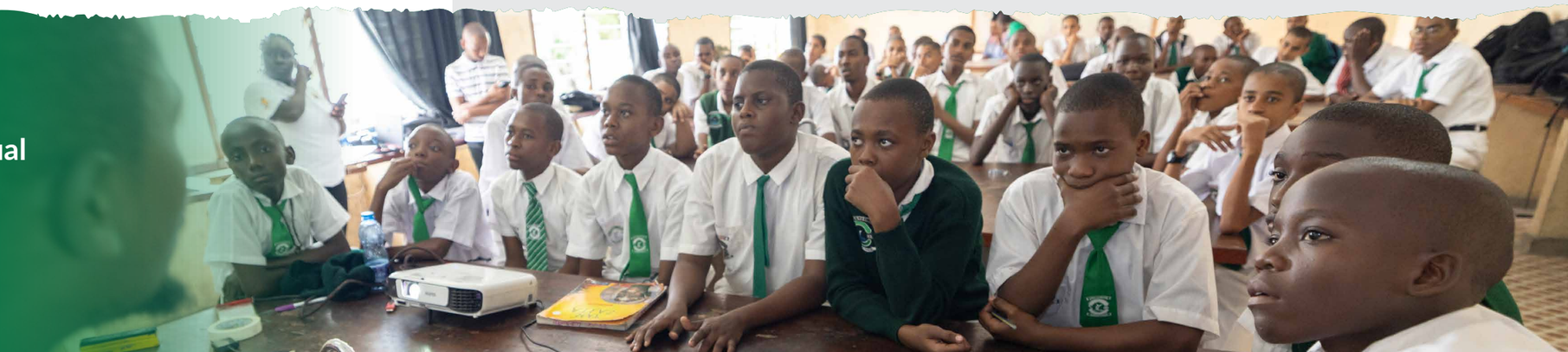
Leadership at the highest level, first and foremost, is crucial to fight against all forms of violence against children, including online child sexual exploitation and abuse. The Namibian President Hage Geingob, while commemorating the International Day of the African Child, recently addressed the growing problem children face in the digital environment and highlighted the urgent need to safeguard the rights of children in the digital environment.[33] The president also urged for a collaborative approach to addressing the online child sexual abuse and exploitation. Such kinds of messages from political leaders are a manifestation of political commitment and help strengthen collaboration and coordination to combat OCSEA.

Many countries in Africa have a dedicated government structure/ministry responsible for child protection broadly.[34] Some others establish multi-sectoral committees dealing with child protection issues, broadly. Multi-sectoral coordination bodies on OCSEA are usually part of this broader national child protection system, and not a separate parallel structure. In Madagascar, for example, the unit that coordinates issues related to online child sexual exploitation and abuse is a multisectoral online protection sub-committee and it is placed within the National Child Protection Committee.[35] While these structures normally aim to address all forms of violence, awareness and technical capacity limitations on OCSEA are evident. Only few African countries, for example, have a dedicated structure/focal person/ taskforce within the overall child protection structure.[36]

On a more positive note, there are countries that offer some good practices. Namibia, for example, is among the few countries which has established a well-functioning multi-sectoral national level coordination structure on child protection. The National Task Force on Child Online Protection was set up in 2016 by the Government of Namibia to oversee the implementation of a national coordinated framework, strategy and roadmap for child online protection. The Task Force is led by the Ministry of Gender Equality, Poverty Eradication and Social Welfare and involves key ministries and agencies such as the Ministry of Safety and Security, the Ministry of Justice, and the Communications Regulation Authority, industry sector stakeholders, CSOs and other partners.[37]

Cross-border collaboration is an important component of the whole child protection system. A key finding across the multiple national studies carried out by 'Disrupting Harm' research project, however, shows the need for stronger cross-border collaboration. Countries, for example, need to link their cybercrime database with INTERPOL's International Child Sexual Exploitation (ICSE) database to benefit from INTERPOL's network and capabilities and better coordinate efforts with other countries. At present, most African countries are not connected with this database.[38] Stronger in-country and cross-national collaboration among governments, law enforcement, ICT sector, INTERPOL and CSO partners working on and with children is required to improve identification of victims, perpetrators and sexual abuse materials, reporting, and effective prosecutions of cases.

The unique nature of online child sexual abuse and exploitation also necessitates cross border cooperation amongst countries, particularly law enforcement.



The WeProtect Global Alliance (WPGA) is an important global/cross-border initiative which brings together governments, civil society organisations and the private sector to better coordinate the global response to child sexual exploitation and abuse online.[39] The Alliance seeks to mobilise important stakeholders at the global level to put an end to online facilitated sexual exploitation and abuse. From Africa, 19 countries have signed up to the WeProtect Global Alliance.[40]

The Internet Watch Foundation (IWF) is another global organisation that is working to find and remove child sexual abuse material (images and videos) from the internet.[41] IWF works with Meta (formerly Facebook), ICMEC (the International Centre for Missing and Exploited Children) and Child Helpline International to raise awareness of the impact of child sexual abuse material, and how its spread can be prevented. In Africa, IWF has launched portals in 23 African countries to receive reports of images and videos that depict child sexual abuse and exploitation. IWF is also working with partners to train law enforcement and child helplines in Africa.[42]

1.3 Programmes and Services

OVERVIEW

Measures in addressing online sexual exploitation of children would broadly constitute steps to protecting children and sentencing and managing sex offenders. Such measures signal efforts to reduce vulnerabilities (of children for online and offline sexual contact, and of CSAM) and reduce demand (for online and offline sexual contact with children, and for CSAM). Each of these approaches requires a series of measures that may involve social protection workers, child protection specialists, law enforcement personnel, educators and others.

Overall, experts suggest the following measures to address OCSEA:[43]

- Awareness creation at a broader societal level and providing therapeutic support to both victims and offenders, including through vulnerability/risk management;
- Taking technical measures through providing online safety, online restrictions or verification methods;
- Disrupting harm by reducing re-victimization, removing CSAM material from the internet and preventing distribution;
- Undertaking crisis response measures to reduce harm by a proactive identification of at-risk children and recovering children are a critical element, mainly by quickly disrupting the progress from initial contact to crisis;
- For offenders, pursuing the criminal justice route whereby perpetrators are translated into justice as well as being provided with therapeutic and rehabilitation support, including in order to avoid reoffending; and
- Undertaking localized studies that cut across the criminal justice and child protection sectors in order to analyze victim and offender behaviour and for contextualizing the above broad measures.

PREVENTATIVE PROGRAMMES AND SERVICES

Prevention is key. One of the most important preventative measures is knowledge and awareness on online child sexual exploitation and abuse. Awareness-raising and education programmes targeting communities at all levels are critical to prevent online child sexual abuse and exploitation. Societal awareness around OCSEA in Africa is low.[44] Communities, governments, policymakers, law enforcement agencies, businesses, and even the families of victims and survivors themselves lack awareness and understanding on how to tackle issues of online safety.[45]

The internet, telecommunications and ICT industry has a special (corporate) social responsibility to influence legislation and policy making, raise awareness and educate the public about cybercrimes, safety risks to children, and develop industry standards and technological solutions to safeguard children online. Yet, there is a dearth of innovative practices by the industry to improve the protection of children from online harm.[46]

Acknowledging the role of the media in raising awareness among the general public, professionals and policy makers, the African Union had included in its OCSEA action plan for 2021 the provision of capacity building programmes to the media on ethical, informed and balanced reporting that is sensitive to a victim's dignity and use of appropriate and universally agreed terminologies around online child sexual exploitation and abuse.[47]

1.2: Four levels of prevention of OCSEA:

- ***Primary prevention***, targeting whole populations including through public sensitization on online safety, awareness programmes and removal of child sexual abuse materials
- ***Secondary prevention***, targeting at-risk groups including the provision of support services for those at risk of offending or victimisation
- ***Tertiary prevention***, targeting those already identified as having a problem including offender treatment programmes and victim support
- ***Quaternary prevention***, which focuses on preventing the negative consequences of counter-measures. For OCSEA, this can include self-harm or suicide prevention for those arrested, minimising vicarious trauma to practitioners exposed to CSAM, and the protection of young victims from potentially traumatic criminal justice procedures

Source: *Baines, V. 2018. Online Child Sexual Exploitation: Towards an Optimal International Response. SSRN Electronic Journal · August 2018*

33 **Number of child helplines across 31 countries in Africa that are members of the Child Helpline International network.**

The participation of children to influence policy and practice relating to child sexual exploitation and abuse is a critical aspect prevention. Children need to be informed and empowered to protect themselves from child sexual abuse. Child participation in all child protection work, however, remains "unstructured and ad-hoc."[48]

An equally important preventative measure is offender management support (in terms of medical, psychological or social support). This kind of support is required not just for convicted offenders but also children displaying harmful sexual behaviors.[49] Data is scanty when it comes to availability of offender management in Africa.

Overall, 35 Member States do not have systems in place in terms of national education programmes for raising awareness, provision of offender management supports, empowerment to children to protect themselves or support to parents, carers, teachers and childcare professionals to keep children safe.[50]

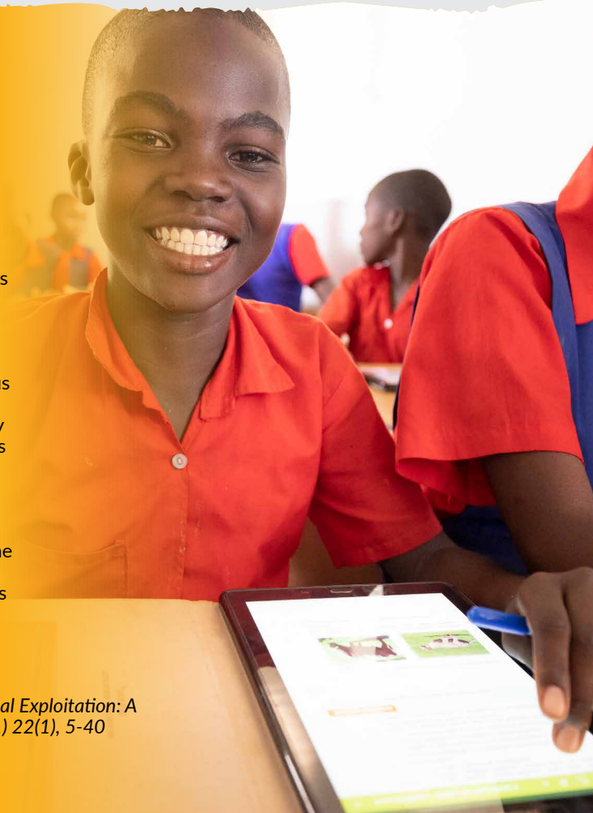
1.3: The role of technology in combatting OSEAC

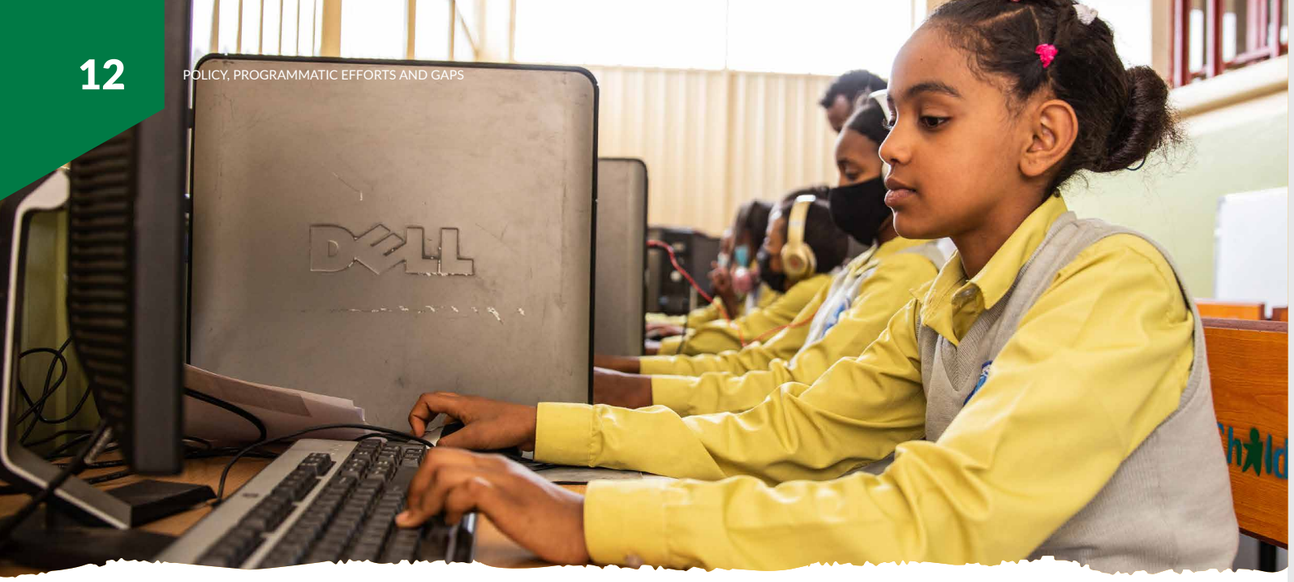
Technology is not only used by those who break the law, but also by those trying to uphold it and pursue offenders. Various technology-reliant core law enforcement efforts are available mostly in developed countries. These include network monitoring systems, data filtering systems, systems developed to triage and prioritize the severity of images and offenders, risk-assessment tools, and specialist digital forensics.

Other measures include image analytics, trust and digital identity, deconstructing the dark side of social media, the study of online underground markets, and cybermoney laundering. A more targeted focus on the handling of digital forensics in the context of online child sexual exploitation and abuse is also necessary. Enabling user-controlled privacy in relation to mobile phones and creating privacy-enhancing technologies (PETs) and cyber-awareness are also important considerations.

Furthermore, there are ongoing efforts in some countries where cybercrime agents and online vigilantes conduct impersonations of children themselves in order to expose offenders. Experts note that, in the future, machine learning or AI-based chatbots may take over the role of undercover cybercrime agents posing as children online. AI developments might assist police if autonomous software-based cybercrime agents could be launched online, attempting to converse with/expose offenders autonomously before referring them for a manual cybercrime review.

Source: *Dionysios S. Demetis, D.S and Kietzmann, J. 2021. Online Child Sexual Exploitation: A New MIS Challenge Journal of the Association for Information Systems (2021) 22(1), 5-40*





RESPONDING TO ONLINE CHILD SEXUAL EXPLOITATION AND ABUSE

While prevention needs to be the primary focus, responsive programmes and services are also required once violations happen. Specialised victim supports, such as reparations, medical or psychosocial support, are needed for healing children subjected to online sexual abuse and exploitation. The research by African Union reveals that 27 African countries had no capability and only 2 member states achieved requirements of this capability. There is limited information on availability of compensation and remedies for victims of OCSEA.

Child helplines play a critical role in the fight against child sexual abuse and exploitation by connecting victims and families with support services. They also allow people to report illegal activities, including the production, procession and distribution of child sexual abuse material or imagery.[51] There are 33 child helplines across 31 countries in Africa that are members of the Child Helpline International network.[52] While these helplines are helping victims and families, there also have challenges. For one thing, lack of awareness, human and financial resources of helplines mean that most of these helplines cannot provide adequate, accessible and quality care to children everywhere in Africa. Most helpline workers are also not trained to provide the support children subjected to OCSEA require. Besides, children's reporting is low as they prefer to disclose to people they know and trust. [53]

The role of the criminal justice system in a coordinated national response cannot be overstated.[54] A strong criminal justice system involves knowledgeable and trained law enforcement, judiciary and prosecutors. Online sex offences – like other cybercrimes - are very difficult to investigate and prosecute because of the difficulty of identifying perpetrators or because of the reluctance of victims to report offences or lack of awareness if those acts are violations that warrant reporting.[55] Law enforcement needs to have the knowledge, skills, tools and resources to lead, support and coordinate investigations. Judges and Prosecutors need to also have the appropriate skills and knowledge on how to handle cases of child sexual abuse and exploitation to enable them perform child-sensitive investigations and secure positive judicial outcomes.

AU's assessment, however, revealed that African countries lag far behind in terms of criminal justice capability on OCSEA.[56] INTERPOL, in many countries, are playing critical roles in supporting national law enforcement organs on cross-border crimes, including OCSEA.

Not many countries in Africa have a dedicated cybercrime law enforcement unit that specifically investigates and prosecutes crimes related to OCSEA.[57] Even when there are units that investigate crimes against children, including child sexual abuse and exploitation, these units do not always have the necessary technical capacity and resources to operate efficiently.[58] A recent study that examined the dynamics of OCSEA in the Economic Community of West African States (ECOWAS) region (with case studies in Ghana, Côte d'Ivoire and Cape Verde) revealed that lack of funding, human resources and technical capacity as well as high turnover of skilled personnel significantly deterred victim identification and reporting on OCSEA issues.[59]

There are a few documented efforts by law enforcement organs around improved capacities and outcomes in carrying out investigations and prosecutions on OCSEA cases. Ghana's effort in this regard is commendable. Following its The Cybersecurity Act 2020, Ghana has established a National Cybersecurity centre within the Ministry of Communications to regulate the cybersecurity activities in Ghana and coordinate the development of cybersecurity across Ghana. The Centre has its own Child Online Protection Unit dedicated to lead responses to OCSEA in close collaboration and coordination with other Ministries, such as the Ministry for Gender, Children and Social Protection, the Ministry of Education and the Ghana Police Service.[60] The centre has already received reports on publication of non-consensual sexual images (sextortion), among others.[61]

South Africa has also done commendable work in investigating OCSEA related cases, conducting forensic investigations and prosecuting these crimes. According to the report by The INTERPOL National Central Bureau Pretoria, between 2017 and 2019, out of 325 reported cases of sexual offences that have online component, South African prosecutors were able to launch 169 investigations and arrested 51 suspected offenders. [62]

Ghana has also reported some successful measures in terms of strengthening its capacity to investigate and prosecute OCSEA cases. In 2020, the Ghana Policy Service launched a child protection digital forensic laboratory which serves to investigate cybercrimes including OCSEA. The lab works closely with different national law enforcement units and INTERPOL whose ICSE database is connected with the lab. With the support of UNICEF, the lab benefited from capacity building training programmes for its police officers on cybercrimes including online child sexual abuse and exploitation.[63] Similarly, Côte d'Ivoire has a dedicated digital forensics laboratory to detect and investigate OCSEA and remove CSEAM.

Apart from law enforcement, the judiciary and prosecutors are key when responding to OCSEA cases. Their knowledge and capacity when it comes to cybersecurity and tackling OCSEA issues is critical for effective response. The reality on the ground, however, is different. Law enforcement and justice professional in many African countries lack the knowledge and the capacity as well as the resources to support children subjected to online sexual abuse and exploitation.[64] There is inadequate information on the provision of capacity building training programmes to these frontline workers.

1.4 Data collection and monitoring systems

Empirical evidence is key to raise awareness, track progress, identify gaps and keep the fight against online child sexual exploitation and abuse. While research in this area is growing, it still remains extremely limited. Little evidence, for example, exists on the scale and magnitude of the impact of the digital environment on the rights of children in Africa and documentation of good practices and solutions that ensure children stay safe online. [65]

A multi-country study called 'Disrupting Harm' is the primary source of evidence to date on the scale, nature and context of online child sexual exploitation and abuse in Africa and a few other regions. So far from Africa, evidence has been generated in a few countries in Eastern and RECs Africa (Ethiopia, Kenya, Mozambique, Namibia, South Africa, Tanzania, Uganda)[66] on the extent of the problem, the risks children face online, how they develop, how they interlink with other forms of violence and what is being done to prevent and reduce them at national level.

Despite the challenges, there are some good practices not just in building the evidence base but also using evidence to inform action on the ground. Ghana's Child Online Protection Framework (2019) and the Cybersecurity Act (2020) which are important instruments to ensuring online safety of children were informed by evidence of gaps and hence have specific and well-defined measures and actions that seek to address identified gaps.[67]

2. Conclusion

Sexual abuse and exploitation of children, be it online or offline, is a form of violence against children that needs to be eliminated. It is, thus, important to look at online child sexual exploitation and abuse (OCSEA) within the broader effort of addressing all forms of violence, including child sexual abuse and exploitation. This does not mean OCSEA does not have specific features that are distinct from offline forms of violence. However, the overlap between online and offline forms of sexual abuse and exploitation needs to be acknowledged while specific strategies are designed to address the specific features of online forms of violence. This will help avoid the risk of establishing parallel structures and systems. This policy brief, by distilling the available evidence on the issue, seeks to call upon all relevant stakeholders to appreciate the urgency, gravity and ubiquity of the problem of online child sexual exploitation and abuse and take the necessary action at various levels.

51

suspected offenders arrested between 2017 and 2019, out of 325 reported cases of sexual offences that have online component in South Africa. Prosecutors were able to launch 169 investigations, according to the report by The INTERPOL National Central Bureau Pretoria.

3. Recommendations

The policy recommendations below are aimed at strengthening existing and ongoing efforts by the various stakeholders to end online sexual exploitation and abuse of children: the AU and its organs, including ACERWC, Regional Economic Communities (RECs), national governments, CSOs, and the private sector (particularly the tech industry), all of which are working towards formulating and influencing policies and action on OCSEA in Africa.

1. **Raising awareness:** OCSEA in Africa is an issue that is not adequately known by policy makers, practitioners, children, families and the general public. It is important for all stakeholders to work towards improving public awareness about what constitutes online child sexual exploitation, the available educational programmes and services, the consequences for violation, and the support systems that are available. Awareness of existing policy provisions and gaps is also critical for policy and law formulations and/or policy reform. It is also important to create broader awareness about structural violence that creates environments which condone violence, in whatever form, or blame the 'victim' or those attitudes and practices that allow potential victims to remain vulnerable and hidden.

2. **Adopting/Strengthening laws and policies:** Adopting legislations that explicitly prohibit online child sexual exploitation and abuse (ratifying international and regional treaties but also harmonising them with local laws and developing OCSEA specific legislations) are all important. It is also important to adopt appropriate regulatory frameworks to hold businesses accountable where they are involved in online sexual abuse and exploitation.

   Legislations need to clearly and comprehensively define OCSEA. Legal provisions need to be adopted regarding reporting and take-down procedures of child sexual abuse material for the online service providers, and criminalization of all forms of online child sexual exploitation and abuse (possession and distribution of child sexual abuse material, grooming of children for sexual abuse and exploitation, including through ICT, cyberstalking and sexual extortion, and live-streaming of child sexual exploitation or abuse).

3. **Implement and enforce laws and policies on OCSEA:** An important aspect of implementation is the allocation of adequate financial resources as well as and technological capabilities to ministries, departments and agencies involved in and responsible for tackling OCSEA. The financial and technological capacity of the police and intelligence agencies needs to be enhanced to conduct as well as act on intelligence and investigate OCSEA related crimes, pursue leads and referrals from international organisations such as INTERPOL and others.

   Prosecutors, judges/magistrates, lawyers, and frontline workers require resources to deliver on their respective mandates and responsibilities. Policy commitments to providing comprehensive support to victims of OCSEA should also be accompanied by investments in free legal aid, temporary housing, psychological services, and other kinds of victim support.

4. **Strengthening cross-sectoral, cross-regional, and cross-country collaboration:** OCSEA, just like other forms of violence against children, is a multi-sectoral and multi-stakeholder issue of concern. As such, coordination and collaboration among all stakeholders is of paramount importance. At a national level, strengthening multi-sectoral coordination and collaboration is important. Likewise, the functionalities and effectiveness of multi-sectoral governance mechanisms need to be examined and strengthened.

   As an issue that knows no border, cross-border collaboration is required. In this regard, it will be crucial to strengthen existing collaborations with Interpol, the WeProtect Global Alliance, the Internet Watch Foundation and others.

5. **Building capacities of professionals:** It is important for police officers, prosecutors, judges/magistrates, lawyers, courtroom staff, statutory social workers, and frontline social workers professionals to have adequate knowledge and technical capacity to provide identify and prosecute perpetrators, as well as provide child-friendly support to victims of online sexual exploitation and abuse. Developing and implementing capacity building training programmes, in collaboration with key stakeholders such as Interpol, is an important step.

6. **Harnessing technological innovations and solutions:** The industry- particularly the technology, telecommunications and ICT sectors- bear special responsibilities in the fight against OCSEA. Deterrence should be prioritised. In this regard, developing tech solutions that include safety by design and similar other initiatives that make it harder for offenders to exploit online services are required. It is more than deterrence of potential offenders. Prevention is all of this, and more.

7. **Data and evidence:** Given the fast evolving nature of technologically facilitated sexual abuse and exploitation against children, it is important to ensure empirical research studies are done systematically and regularly on the scale, magnitude and impact of the problem but also on good practices that can be adopted and implemented at a scale. While there are various efforts to generate evidence already, it is important to ensure research studies lead or inform or be used by governments to develop national response strategies and plans.

Endnotes

1 Access Now. 2022. Weapons of Control, Shields of Impunity: Internet Shutdowns in 2022. Available at: https://www.accessnow.org/
2 ACERWC. 2023. Concept Note: Day of the African Child 2023: THE RIGHTS OF THE CHILD IN THE DIGITAL ENVIRONMENT. Available at: https://www.acerwc.africa/
3 African Union.2020. Strengthening Regional and National Capacity and Action against Online Child Sexual Exploitation and Abuse in Africa Strategy and Plan of Action 2020 – 2025. African Union. Addis Ababa
4 https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation
5 https://www.acerwc.africa/en/page/agenda-2040
6 African Union. List of Countries Which Have Signed, Ratified/Acceded to The African Union Convention on Cyber Security and Personal Data Protection. Available at: https://dataprotection.africa/wp-content/uploads/2305121.pdf
7 African Union. 2020. ONLINE CHILD SEXUAL EXPLOITAITION AND ABUSE (OCSEA). Strengthening Regional and National Capacity and Action against Online Child Sexual Exploitation and Abuse in Africa. Strategy and Plan of Action 2020 – 2025. Accessed at: https://au.int
8 https://au.int/en/pressreleases/20191212/communique-global-summit-tackle-online-child-sexual-exploitation
9 Communique of the Global Summit to Tackle Online Child Sexual Exploitation. 2019. Protecting Children from Abuse in the Digital World. Available at: https://au.int/
10 African Union. 2020. ONLINE CHILD SEXUAL EXPLOITAITION AND ABUSE (OCSEA). Strengthening Regional and National Capacity and Action against Online Child Sexual Exploitation and Abuse in Africa. Strategy and Plan of Action 2020 – 2025. Accessed at: https://au.int
11 General Comment No. 7 on article 27 on Sexual Exploitation of the African Charter on the Rights and Welfare of the Child. Accessed at: https://www.acerwc.africa/sites/default/files/2022-09/General-Comment-on-Article-27-of-the-ACRWC_English_0.pdf
12 33rd Session of the ACERWC. 2019. Available at: https://www.acerwc.africa/sessions/
13 ACERWC. 2019. Report of the 33rd Ordinary Session of the African Committee of Experts on the Rights and Welfare of the Child (ACERWC). Available at: https://www.acerwc.africa/en
14 https://www.eac.int/
15 International Telecommunication Union 2013. Computer Crime and Cybercrime: Southern African Development Community (SADC) Model Law
16 https://ecowas.int/
17 African Union.2020. Strengthening Regional and National Capacity and Action against Online Child Sexual Exploitation and Abuse in Africa Strategy and Plan of Action 2020 – 2025. African Union. Addis Ababa
18 United Nations Children's Fund. 2021. Ending online child sexual exploitation and abuse: Lessons learned and promising practices in low- and middle-income countries. New York
19 ACERWC. 2021. General Comment No. 7 on article 27 on Sexual Exploitation of the African Charter on the Rights and Welfare of the Child
20 Institute of Health Economics 2010. Sexual Exploitation of Children and Youth Over the Internet: A Rapid Review of the Scientific Literature
21 Dalins, J., Wilson, C., & Carman, M. (2018). Criminal motivation on the dark web: A categorisation model for law enforcement. Digital Investigation, 24, 62–71.
22 Ibid
23 UNICEF Office of Research – Innocenti. 2022. Online Risk and Harm for Children in Eastern and Southern Africa. Available at: www.unicef.org
24 African Union.2020. Strengthening Regional and National Capacity and Action against Online Child Sexual Exploitation and Abuse in Africa Strategy and Plan of Action 2020 – 2025. African Union. Addis Ababa
25 Kenya, The Children Act 29 of 2022, arts. 2 and 22(3), (4).
26 United Nations Children's Fund (2021) Ending online child sexual exploitation and abuse: Lessons learned and promising practices in low- and middle-income countries, UNICEF, New York
27 ECPAT, INTERPOL, and UNICEF. (2022). Disrupting Harm in South Africa: Evidence on Online Child Sexual Exploitation and Abuse. Global Partnership to End Violence against Children
28 https://www.iwf.org.uk/news-media/news/new-reporting-portal-to-address-critical-need-to-keep-children-safe-in-ghana/
29 https://www.itu.int/ITU-D/projects/ITU_EC_ACP/hipssa/Activities/SA/docs/SA-1_Legislations/Botswana/CYBERCRIMES.pdf
30 Botswana Children's Act 2009. Available at: http://jafbase.fr/docAfrique/Botswana/Children%20act.pdf
31 WeProtect Global Alliance. The Model National Response. Available at: https://www.weprotect.org/model-national-response/
32 Ibid
33 https://english.news.cn/20230616/52f55117e5c145db8e7cff47f7128996/c.html
34 African Union.2020. Strengthening Regional and National Capacity and Action against Online Child Sexual Exploitation and Abuse in Africa: Strategy and Plan of Action 2020 – 2025. African Union. Addis Ababa
35 United Nations Children's Fund. 2021. Ending online child sexual exploitation and abuse: Lessons learned and promising practices in low- and middle-income countries, UNICEF, New York
36 Ibid
37 Source for the above: United Nations Children's Fund. 2021. Ending online child sexual exploitation and abuse: Lessons learned and promising practices in low- and middle-income countries, UNICEF, New York
38 ECPAT and Interpol. 2018. Towards a Global Indicator on Unidentified Victims in Child Sexual Exploitation Material: Technical Report. Available at: https://www.interpol.int/en/Crimes/Crimes-against-children/International-Child-Sexual-Exploitation-database
39 https://www.weprotect.org/alliance/
40 The 19 AU member states who signed up to the alliance are: Angola, Burundi, Central African Republic, Ethiopia, Ghana, Republic of Guinea, Kenya, The Kingdom of Lesotho, Malawi, Namibia, Nigeria, Rwanda, Senegal, Sierra Leone, South Africa, Sudan, Tanzania, Uganda and Zambia.
41 https://www.iwf.org.uk/
42 https://childhelplineinternational.org/iwf-works-with-meta-icmec-and-child-helpline-international-on-a-new-campaign-against-child-sexual-abuse-in-africa/

43 Online Child Sexual Exploitation: Towards an Optimal International Response Victoria Baines SSRN Electronic Journal · August 2018

44 UNICEF Office of Research – Innocenti. 2022. Children's Experiences of Online Sexual Exploitation and Abuse in 12 Countries in Eastern and Southern Africa and Southeast Asia. Disrupting Harm Data Insight 1. Global Partnership to End Violence Against Children.

45 Hoang, Thi and Wagneretp, Livia. 2023. Online child sexual exploitation and abuse in West Africa. Organised Crime: West African Response to Trafficking. Available at: https://globalinitiative.net/wp-content/uploads/2023/08/OCWAR-T-PB-7.pdf

46 African Union.2020. Strengthening Regional and National Capacity and Action against Online Child Sexual Exploitation and Abuse in Africa Strategy and Plan of Action 2020 – 2025. African Union. Addis Ababa

47 AUC. OSCEA Programmatic Response Plan for 2021. Available at: https://au.int/

48 African Union.2020. Strengthening Regional and National Capacity and Action against Online Child Sexual Exploitation and Abuse in Africa Strategy and Plan of Action 2020 – 2025. African Union. Addis Ababa

49 WeProtect Global Alliance. Model National Response. Available at: https://www.weprotect.org/model-national-response/

50 Ibid

51 https://www.icmec.org/hotlines-and-helplines/

52 https://childhelplineinternational.org/africa-fit-for-children/

53 UNICEF Office of Research – Innocenti. 2022. Children's Experiences of Online Sexual Exploitation and Abuse in 12 Countries in Eastern and Southern Africa and Southeast Asia. Disrupting Harm Data Insight 1. Global Partnership to End Violence Against Children.

54 WeProtect Global Aliance.2016. Preventing and Tackling Child Sexual Exploitation and Abuse: A Model National Response (MNR). Accessed at: https://www.weprotect.org/

55 internet Emma A. Jane and Elena Martellozzo Introduction Victims of cybercrime on the small 'i', Martellozzo, E. and Jane, E.A. eds. Cybercrime and its victims.

56 African Union.2020. Strengthening Regional and National Capacity and Action against Online Child Sexual Exploitation and Abuse in Africa Strategy and Plan of Action 2020 – 2025. African Union. Addis Ababa

57 ACERWC. 2021. General Comment No. 7 on article 27 on Sexual Exploitation of the African Charter on the Rights and Welfare of the Child

58 African Union.2020. Strengthening Regional and National Capacity and Action against Online Child Sexual Exploitation and Abuse in Africa Strategy and Plan of Action 2020 – 2025. African Union. Addis Ababa

59 Hoang, Thi and Wagner, Livia. A growing threat? Online child sexual exploitation and abuse in Ghana, Côte d'Ivoire and Cape Verde, OCWAR-T Research Report 7. Available at: https://globalinitiative.net/

60 United Nations Children's Fund. 2021. Ending online child sexual exploitation and abuse: Lessons learned and promising practices in low- and middle-income countries, UNICEF, New York

61 https://www.csa.gov.gh/cert-gh

62 ECPAT, INTERPOL, and UNICEF. 2022. Disrupting Harm in South Africa: Evidence on Online Child Sexual Exploitation and Abuse. Global Partnership to End Violence against Children.

63 United Nations Children's Fund. 2021. Ending online child sexual exploitation and abuse: Lessons learned and promising practices in low- and middle-income countries, UNICEF, New York

64 UNICEF Office of Research – Innocenti. 2022. Children's Experiences of Online Sexual Exploitation and Abuse in 12 Countries in Eastern and Southern Africa and Southeast Asia. Disrupting Harm Data Insight 1. Global Partnership to End Violence Against Children.

65 Ibid

66 Disrupting Harm. Accessed at: https://ecpat.org/disrupting-harm/

67 Republic of Ghana, Ministry of Communications and Digitalisation, 'Cybersecurity Act Passed to Promote & Regulate Cybersecurity Activities' <https:// www.moc.gov.gh/cybersecurity-act-passed-promote-regulate-cybersecurity-activities.

ChildFund®
Because we need each other.

www.childfund.org

African Child Policy Forum ACPF

www.africanchildforum.org

A JOINT PUBLICATION OF CHILDFUND INTERNATIONAL AND THE AFRICAN CHILD POLICY FORUM.