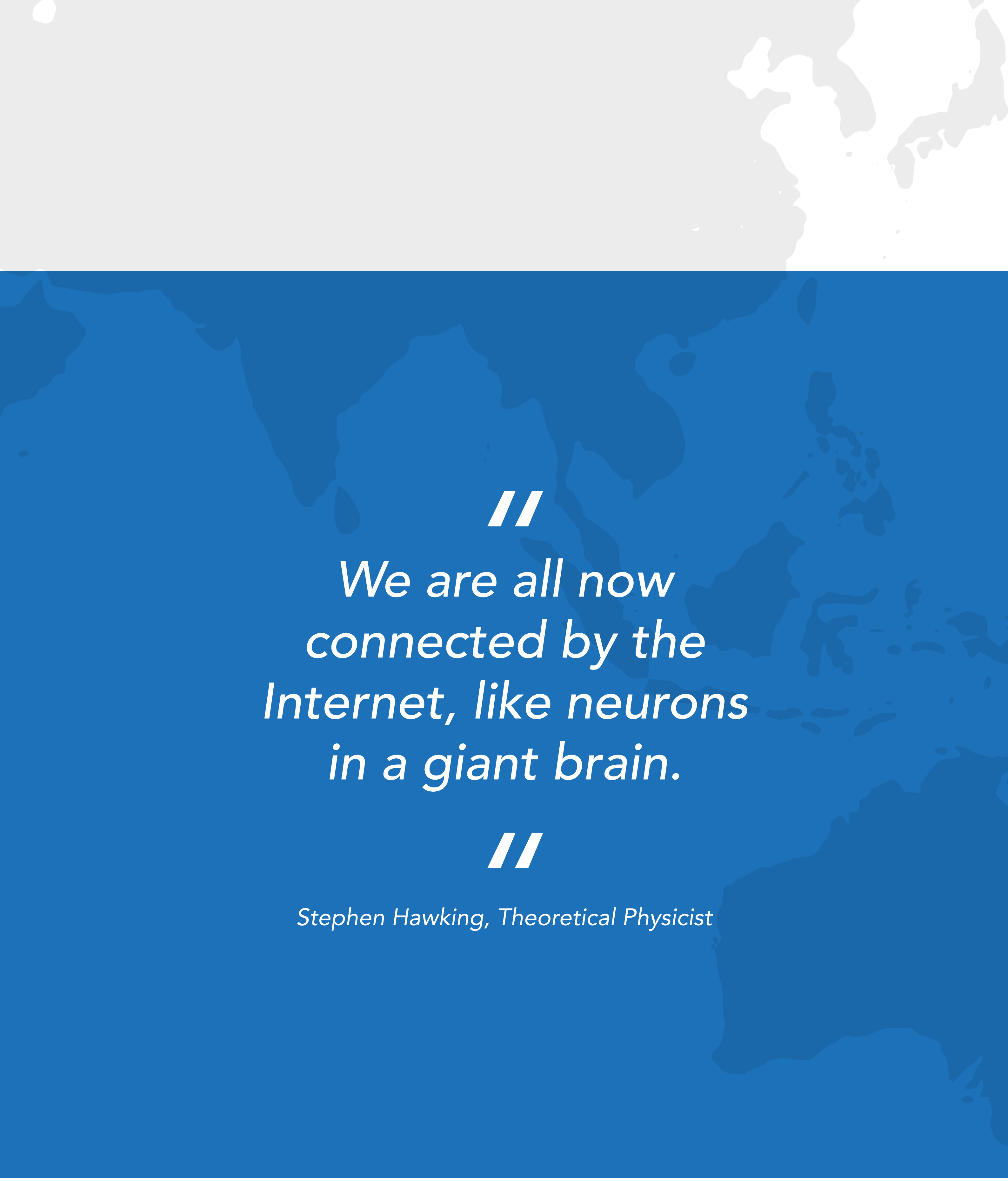
# Africa Safer Internet Day 2021

Theme:

## Positioning and Partnering for Child Online Protection.

#ASID2021

# Table of Content



> "
>
> *We are all now connected by the Internet, like neurons in a giant brain.*
>
> "

*Stephen Hawking, Theoretical Physicist*

# About Africa Safer Internet Day (ASID)

At the Accra Forum on Child Online Protection in October 2019, member states resolved that effective 2020 the International Telecommunications Union's Regional Office for Africa should mobilize for the Africa Safer Internet Day (ASID) celebration on the continent. This will enable the choice of theme for the celebration to take on board the peculiar and diverse needs of the continent.

Over the years, Safer Internet Day has become a landmark event in the online safety calendar events. The year 2021 will see the 18th celebration with actions across the globe. Started as an initiative of the EU Safe Borders project in 2004 and was taken up by the Insafe network as one of its earliest actions in 2005.

Over the years, Safer Internet Day has grown beyond its traditional geographic zone and is now celebrated in approximately 170 countries worldwide and coordinated by the INSAFE/INHOPE Network. The International Telecommunications Union (ITU) is the leading Specialized Agency of the United Nations, responsible for issues concerning information and communication technologies. ITU is the only international organization which convenes ICT ministries, regulators and industry regularly to fulfil its mandate.

# **Sango** the Mascot for Child Online Protection

**(Rename the mascot for use in your country)**

# The goal of #ASID2021

With the vision of creating a world where children can be connected and can fully benefit from the opportunities of a trusted and safe online environment the ITU has outlined the following goals for Africa:

- Promote an Africa-wide education and awareness on the importance of child online safety.
- Raise awareness with governments, industry, educators, children and parents to ensure that the African Child is safe and secure online while online.
- Design strategies to empower and support the African child's resilience building.
- Develop, share or contextualize available resources to support children’s learning and education.

# What is “COP Initiative and the Guidelines”?

The explosion of information and communication technology has herewith created unprecedented opportunities for children and young people to communicate, connect, share, learn, access information and express their opinions on matters that affect their lives and their communities. But wider and more easily available access to the Internet and mobile technology also poses significant challenges to children’s safety and wellbeing – both online and offline.

To respond to the challenges posed by the rapid development of ICTs and the child protection challenges they bring, the Child Online Protection (COP) Initiative was launched as an international multi-stakeholder platform by the International Telecommunication Union (ITU) in November 2008. In 2009, the first set of guidelines on child online protection were issued by the ITU in the context of the COP Initiative which has become a holistic global blueprint for the protection of children while they make use of online platforms. The ITU Member States reaffirmed the importance of the COP Initiative at the Plenipotentiary Conference of the ITU held in Dubai in 2018. According to Resolution 179 (Rev. Dubai, 2018), ITU in collaboration with the COP initiative partners and stakeholders has been instructed to update all sets of guidelines while taking into consideration technology developments in the telecommunication industry, including guidelines on children with disabilities and children with specific needs.

The current Africa focused set of guidelines was launched in 2020 and recognizes the protection of children online within the framework of international and regional instruments such as the United Nations Convention on the Rights of the Child, African Charter on the Rights and Welfare of the Child, Agenda 2040 and the 2030 Agenda for Sustainable Development, in particular SDGs 1, 3, 4, 5, 9, 10 and 16.

The guidelines are to serve as a reference point and road maps for the development of national level strategies related to Child Online Protection.
In late 2019, the ITU/UNESCO Broadband Commission for Sustainable Development launched the Child Online Safety Report with actionable recommendations on how to make the Internet safer for children.

***https://www.itu.int/en/ITU-D/Regional-Presence/Africa/Pages/Child-Online-Protection-Training--.aspx***

***https://www.broadbandcommission.org/Documents/working-groups/ChildOnlineSafety_Declaration.pdf***

# Who can use the "COP Guidelines"?

Based on the strategic pillars of the COP initiative below, are some stakeholders required at all levels to ensure effective implementation of the national level actions:

- Children and young people
- Parents, guardians, carers and educators
- Government Ministries
- Industry and connectivity providers
- Research and academia
- Non-governmental organizations
- Law enforcement
- Health and Social services
- Others per country-specific needs.

# Why and How was this guide developed?

Guidelines have been co-authored by the ITU and a multi-stakeholder working group of from leading institutions who are active in the area of ICTs as well as in child (including online) protection and rights. The Guidelines represent the first international instrument which aims at applying a holistic approach toward COP on the international level. Thus:

- Provide the first-ever holistic approach to COP with a broad focus on all kinds of risks and harms, but also potential, for children related to the online environment.

- The result of a joint effort of a working group of internationally recognized key experts in the field of child protection, cybersecurity and ICTs.

- Serve as a platform for leaders with a multi-stakeholder community, providing a strong network of partners for validation and joint implementation.

# Partnership for COP guidelines in the national strategy

Basic Facts:

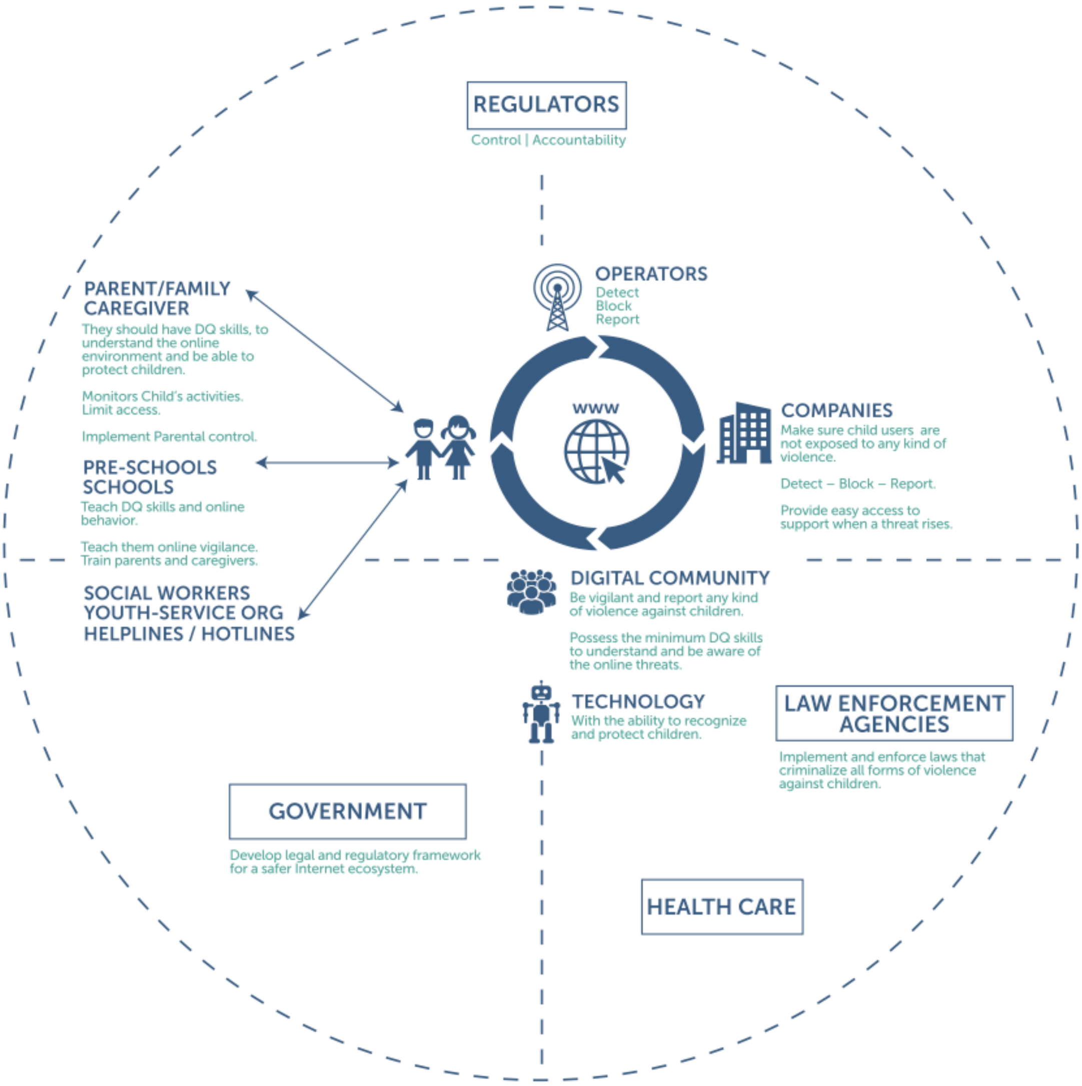
- Each child has a story but the common denominator is; they are being accessed by predators in the own spaces with a keyboard.
- Everyone needs to take RESPONSIBILITY to protect children.
- These devices are used to inflict abuse on children.
- Software Programmes are used to edit the abuse.
- File transfer software will be used to share it.
- Internet platforms and online image stores are used to distribute.
- A group of people create demand.
- Another group meets the supply.
- We all have to STOP this content and protect the African child.

Several partnerships are key to the successful design and development of national COP strategy. Successfully designing and delivering of a National strategy may mean engaging in partnerships with a number organizations. Different partners bring diverse strengths, so depending on the role of the lead organisation and the peculiar needs of the country, priority could be given to the following:

- Partner with Mobile Network Operators.
- Partner with NGOs and local development organizations.
- Partner with government agencies.
- Partner with research organizations and consultancies.

# What is SAFER Internet?

## Safer Internet Ecosystem


REGULATORS
Control | Accountability
OPERATORS
Detect
Block
Report
PARENT/FAMILY CAREGIVER
They should have DQ skills, to understand the online environment and be able to protect children.
Monitors Child's activities. Limit access.
Implement Parental control.
www
COMPANIES
Make sure child users are not exposed to any kind of violence.
Detect – Block – Report.
Provide easy access to support when a threat rises.
PRE-SCHOOLS SCHOOLS
Teach DQ skills and online behavior.
Teach them online vigilance. Train parents and caregivers.
SOCIAL WORKERS
YOUTH-SERVICE ORG
HELPLINES / HOTLINES
DIGITAL COMMUNITY
Be vigilant and report any kind of violence against children.
Possess the minimum DQ skills to understand and be aware of the online threats.
TECHNOLOGY
With the ability to recognize and protect children.
LAW ENFORCEMENT AGENCIES
Implement and enforce laws that criminalize all forms of violence against children.
GOVERNMENT
Develop legal and regulatory framework for a safer Internet ecosystem.
HEALTH CARE

Source: Lina Fernandez del Portillo.

*To fully protect children from online harm or exposure to unacceptable online risk, all relevant stakeholders must be informed, empowered and engaged.*

***https://www.broadbandcommission.org/workinggroups/Pages/WG1-2018.aspx***

| | |
|---|---|
| A future proof and effective legal framework | The critical of education and awareness. |
| A company culture which prioritizes Child Safety. | Making sure the safety of children is a key consideration at the design stage thus: Safety By Design. |
| Empowered children who are aware of their rights. | The deliberate role of Technology in guaranteeing safer space. |

# Addressing Child Online Sexual Exploitation and Abuse Challenges

There are various factors influencing child exploitation and abuse in developing economies. According to an ECPAT report 2018, about 24 countries in Africa are involved in addressing the challenges (Gacengo 2018). However, due to the complexity of the phenomena, there has been little study on COSEA, especially in Africa and this could be attributed to lack of accountability and autonomy on the part of government & the various stakeholders as well as inadequate local policing mechanisms at all levels across the supply chain.

# Understanding Steps Deployed by Perpetrators to Exploit Children Online.

The Perpetrator adopts the following steps to exploit children online including reconnaissance, social engineering or catfishing, grooming, sexting, sextortion and consuming.

***Reconnaissance:*** Perpetrators carryout online searches and visits various online forums to identify which platforms they can join and can conceal themselves and identify vulnerable children.

***Social Engineering or Catfishing:*** Perpetrator uses a false identity, and tricks on the child to reveal personal information about themselves and their families that could be used on the victims.
Grooming: Perpetrators use deceptions to gather intelligence about the child to build emotional relationships, trust, and affection to manipulate, exploit and abuse the victims later.

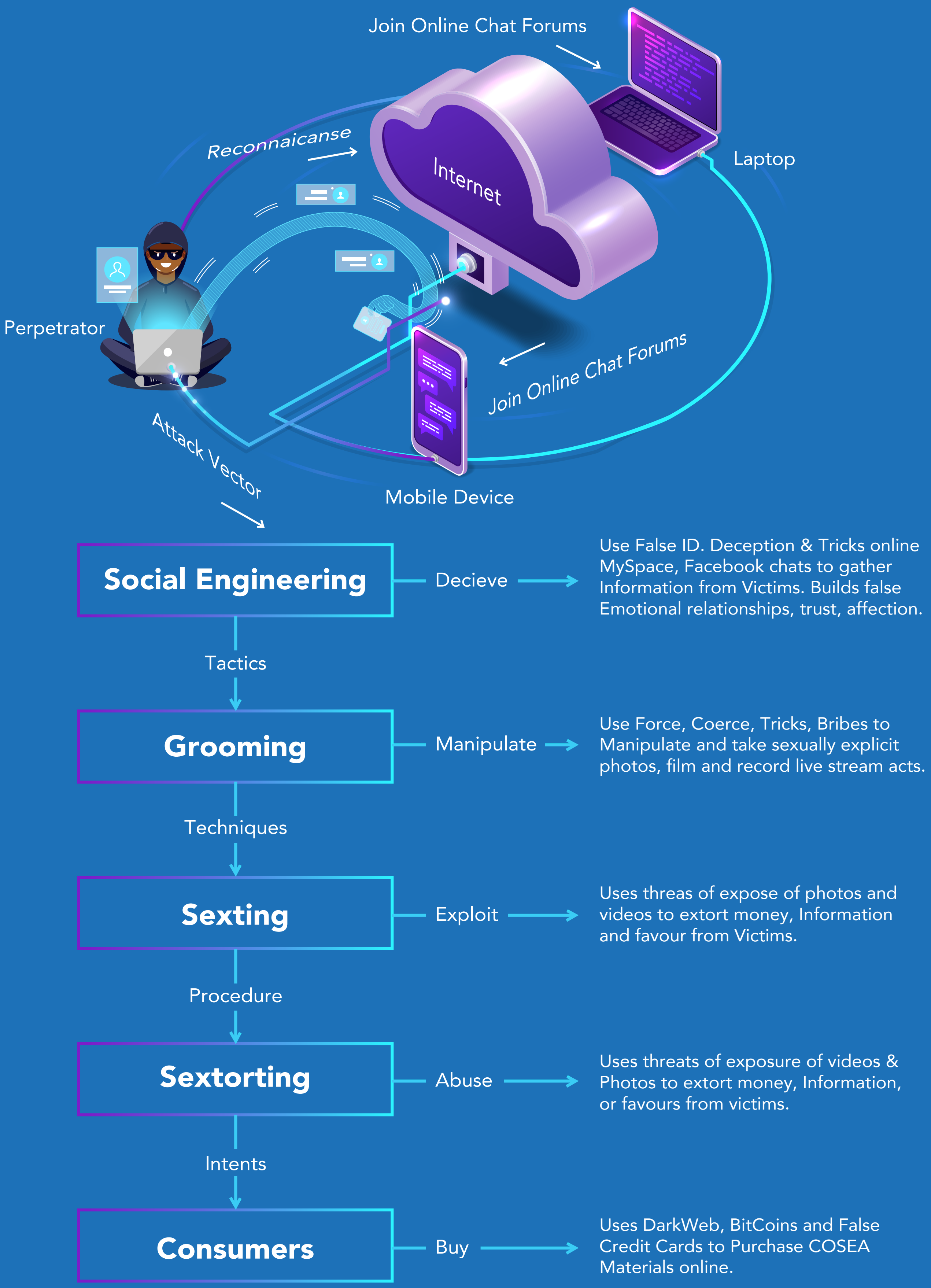
***Sexting:*** Perpetrators use force, bribes, tricks, and persuasion to get the victims online and into sexually explicit acts. They connect via smartphones with webcams to share sexually explicit photos, images and livestreaming of themselves and the child inappropriately either off or online.

***Sextortion:*** Perpetrators use threats to try to extort money, information, or sexual favours from their victims by threatening to reveal their sexually explicit activities that they have secretly recorded unlawfully on social media.

***Consumers:*** Are those who purchase COSEA materials online using false Credit Cards on the Dark Web and Bitcoins.

# Child Online Sexual Exploitation & Abuse Challenges in Africa

COSEA in Africa has been a major challenge due to factors such as inability to categorize victims' characteristics including children's behaviours, online activities, content monitoring that could provide potential opportunities for education, awareness, attitudinal changes, victim support and information sharing platforms.  It is important to understand the Tactics, Techniques and Procedures (TTPs) to appreciate the role of the various stakeholders who should be involved in the local policing mechanism. TTPs provide knowledge and understanding of the pattern of behaviour, social mediums, marketing platform, financial benefits and security related issues that need to be addressed.



**Social Engineering** — Decieve → Use False ID. Deception & Tricks online MySpace, Facebook chats to gather Information from Victims. Builds false Emotional relationships, trust, affection.

Tactics ↓

**Grooming** — Manipulate → Use Force, Coerce, Tricks, Bribes to Manipulate and take sexually explicit photos, film and record live stream acts.

Techniques ↓

**Sexting** — Exploit → Uses threas of expose of photos and videos to extort money, Information and favour from Victims.

Procedure ↓

**Sextorting** — Abuse → Uses threats of exposure of videos & Photos to extort money, Information, or favours from victims.

Intents ↓

**Consumers** — Buy → Uses DarkWeb, BitCoins and False Credit Cards to Purchase COSEA Materials online.

Figure 1. TTPs Deployed on Children online

Several Psychosocial challenges exist in Africa which could be as a result of cultural interrelation of social factors and individual thoughts and behaviours which impact on the increasing cases of COSEA. Further, the roles of the mobile network operators, ISPs and other providers in identifying the offence on their online platforms, payments mediums, apps, websites, and payment platforms that are used by perpetrators to assist in the detection and prevention of victims from their exploits is lacking.

Additionally, the challenge of employing competent personnel in identifying the tactics, techniques, and procedures in committing the cybercrimes, their modes of operations and intents will provide a basis for understanding their motives either, financial, pleasure, extortion, exploitation or revenge.
The concern over child online protections should not be limited to arresting the perpetrators and prosecuting them but should include providing support, mitigation, rehabilitation and counselling that may assist in minimising the harms as recommended in the Child Online Protection Guidelines for Policy Makers and Industry.

Figure 2 below depicts a child-centred approach about the various stakeholders in dealing with COSEA concerns, seeing the child at the centre of all these gives a vivid picture of how the issues are to be addressed. Surrounded by the child online are the various entities, institutions, and stakeholders. Making social services, hospitals, educating children, banks, faith-based institutions, internet cafes, telecommunications and the ISPs, laws and legislatures, parental control, academia, law enforcement, perpetrators and COSEA consumers understand their responsibility towards the child makes it easier to deal with the issue.

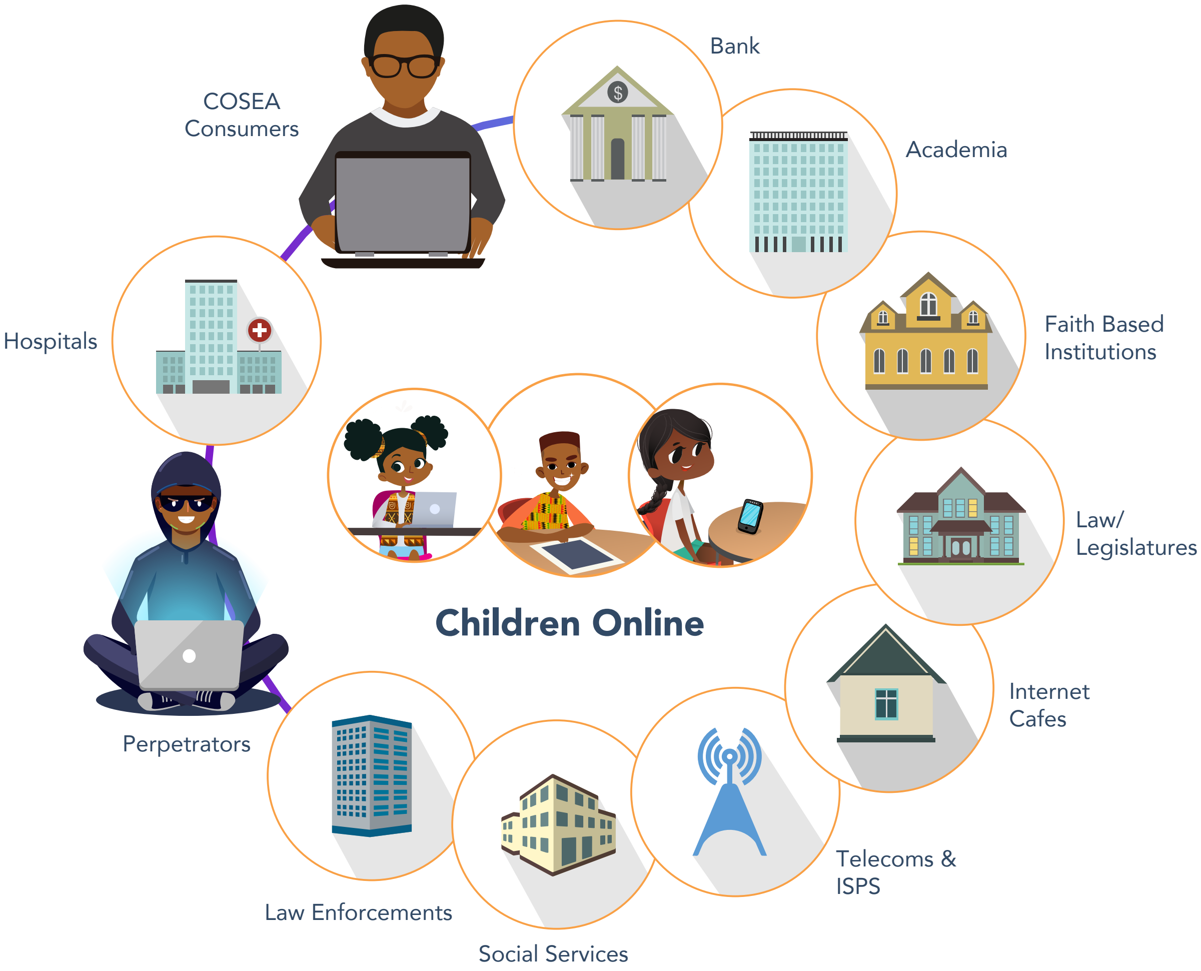


Figure 2. Child Centred Approach to Factors that Influence COSEA Challenges

# What can you do for your country?

- Adapt Songo the Mascot and give it a local name to deliver safety messages to young people in your country.
- Ensure that you have the following in place: Refer to the Policy Makers Guide.
- The following stakeholders should be talking to one another to promote Child Online Safety in your country as stated in the ITU Child Online Protection Guidelines.
- Understanding abuse and knowing where to report is fundamental.
- Build resilience of children and do not ignore the red flags.
- Align issues of Child Online Safety to CP in the physical.
- Liaise with country level regulators, policy makers etc for answers.
- Reach out for resources to update yourself because it is fast-paced.

Further Reading:

*https://www.itu.int/en/ITU-D/Regional-Presence/Africa/Pages/Child-Online-Protection-Training--.aspx*
*www.toolkits.childonlineafrica.org/*
*http://www.sidafrica.childonlineafrica.org/*

# Partners

FACEBOOK

NATIONAL COMMUNICATIONS AUTHORITY

innovaré

AFRICAN TELECOMMUNICATIONS UNION
ATU ★ UAT

World Vision

Ministry of Communications
Republic of Ghana

dimension
data

Safer
Internet
Day

ChildOnline
Africa

Africa
Digital
Rights
Hub

Africa Safer
Internet Day

NCC
NIGERIAN
COMMUNICATIONS
COMMISSION

CBOD
GHANA CHAMBER OF BULK OIL DISTRIBUTORS

**#ASID2021** is funded by:
**NCA, CBOD, Facebook, ADRH, Dimension Data Ltd**
and **Innovare Learning Ltd.**

Contact Person:
**Ida Jallow** - Programme Coordinator
ITU Regional Office for Africa

Email: **ida.jallow@itu.int**

Tel: **+251 11 551 4855/4977**

IP Tel: **+41 22 730 6353**

Website:
***https://www.itu.int/en/ITU-D/Regional-Presence/Africa/Pages/default.aspx***