



COP Africa Programme



ADVANCING ISSUES
1,382 (43%) 512 (35%)
DECLINING ISS
1,143 (39%) 92 (9%)



ADVANCING ISSUES 1,382 (43%) 5 1 2
(38%) 1,143 (39%) 92

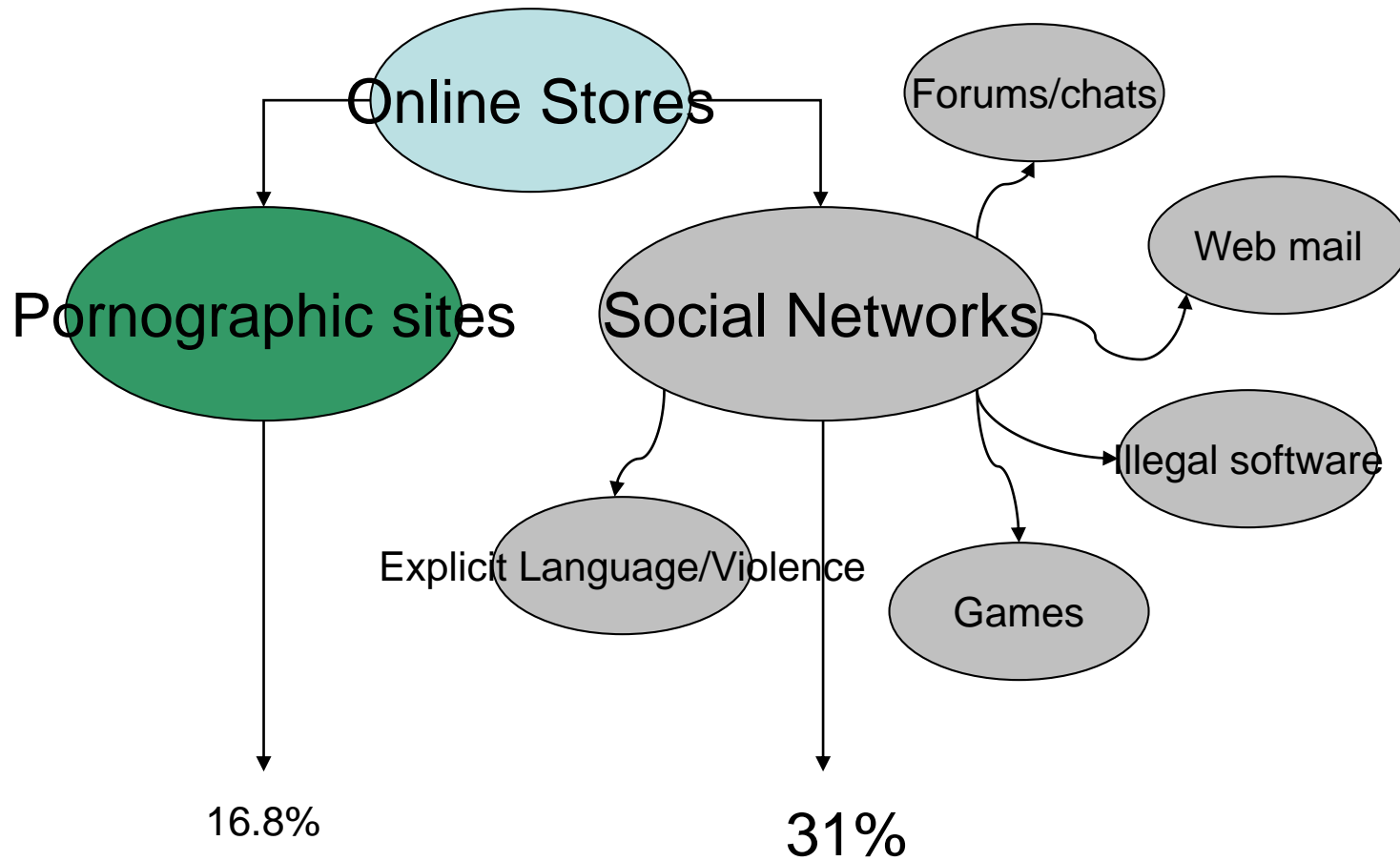
Children and young people online safety and protection



ADVANCING ISSUES 1,382 (43%) 512 (35%) 1,894 (39%) 92
DECLINING ISSUES 1,143 (39%) 92 (9%) 1,861 (37%) 161
UNCHANGED ISSUES 91 (9%) 28 (14%) 91 (9%) 32
TOTAL ISSUES 3,231 1,841 2,885 2
NEW HIGHS 191 28 71 2
UP VOLUME 2,348 409 863 (35%) 172,608,898 (27%) 533,440,318 (29%) 291,292,816
DOWN VOLUME 883 141 928 (28%) 1,487,206 (46%) 1,487,206 (46%)
UNCHANGED VOLUME 1,000 1,000 (100%) 1,000 (100%) 1,000 (100%)
TOTAL VOLUME 3,431 (100%) 2,497 (73%) 2,849 (83%) 1
622,071,624 ADVANCING ISSUES 1,382 (43%) 92 (35%) 1,363 (39%) 92 (38%)
DECLINING ISSUES 1,143 (35%) 913 (82%) 1,661 (57%) 109 (14%)
UNCHANGED ISSUES 91 (9%) 28 (14%) 91 (9%) 32 (35%)
TOTAL ISSUES 3,231 1,841 2,885 2
NEW HIGHS 191 28 71 2
NEW LOWS 191 28 71 2



What Children Are Doing Online

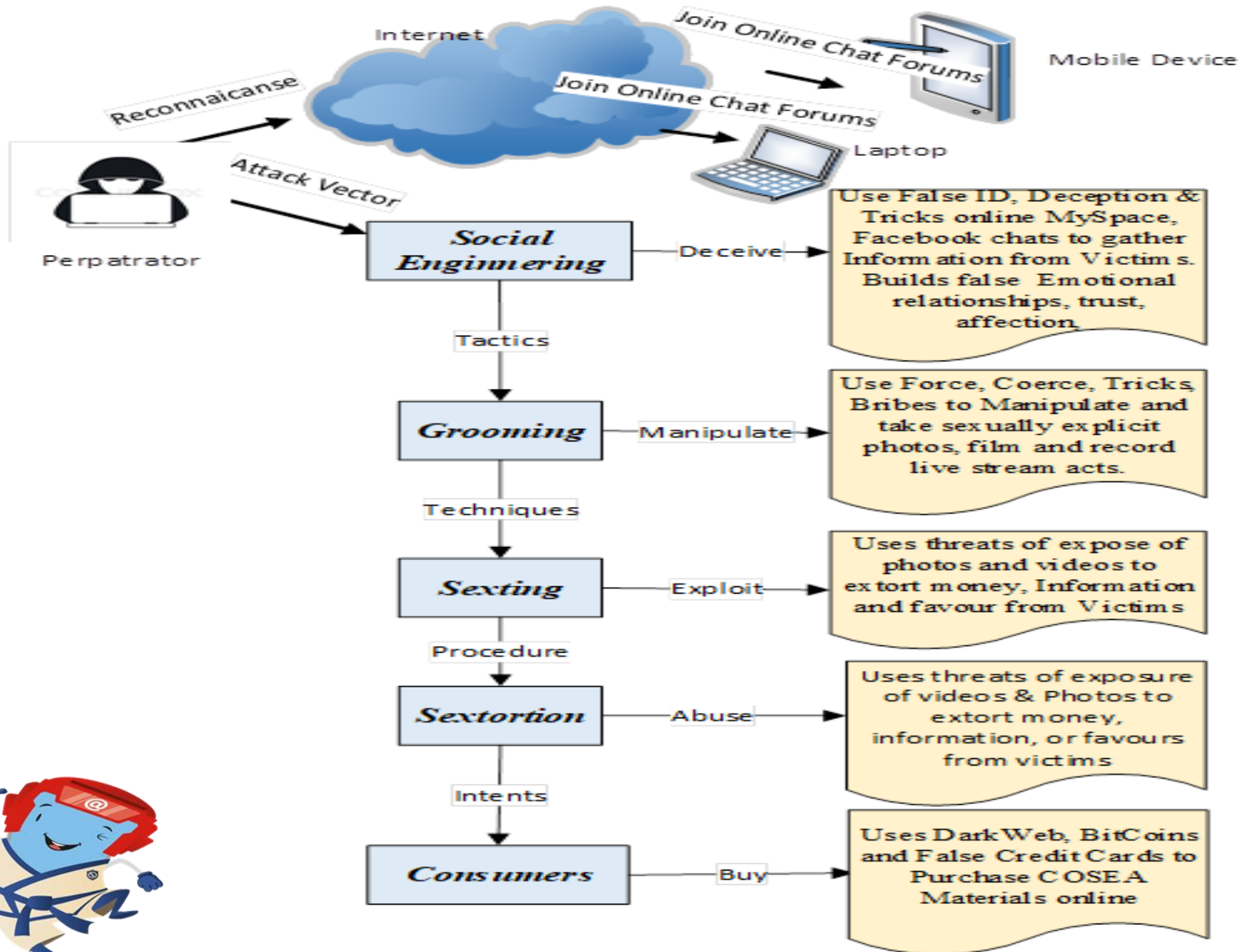


Types of Children who are taken



- Every Child can be a victim of exploitation.
- Children who are depressed.
- Children who might have suffered some form of trauma.
- Children with anti-social behaviours due to abuse.







Individual Vulnerabilities

- **Life events – history of:**

- Poor or chequered of other forms of abuse
- Excessive or addictive use of alcohol, drugs or gambling
- Petty crime
- Financial weaknesses

- **Personal circumstances**

- Sympathy to specific causes/adversarial mindset
- Difficult family circumstances
- Peer pressure

- **Personality predispositions**

- Low self esteem - desire for recognition/status
- 'Thrill seeker' - desire for excitement
- Overinflated sense of worth/abilities – desire for revenge when not recognised
- Brittle - oversensitive, unable to accept criticism – desire for revenge for perceived injustices



Social Engineering

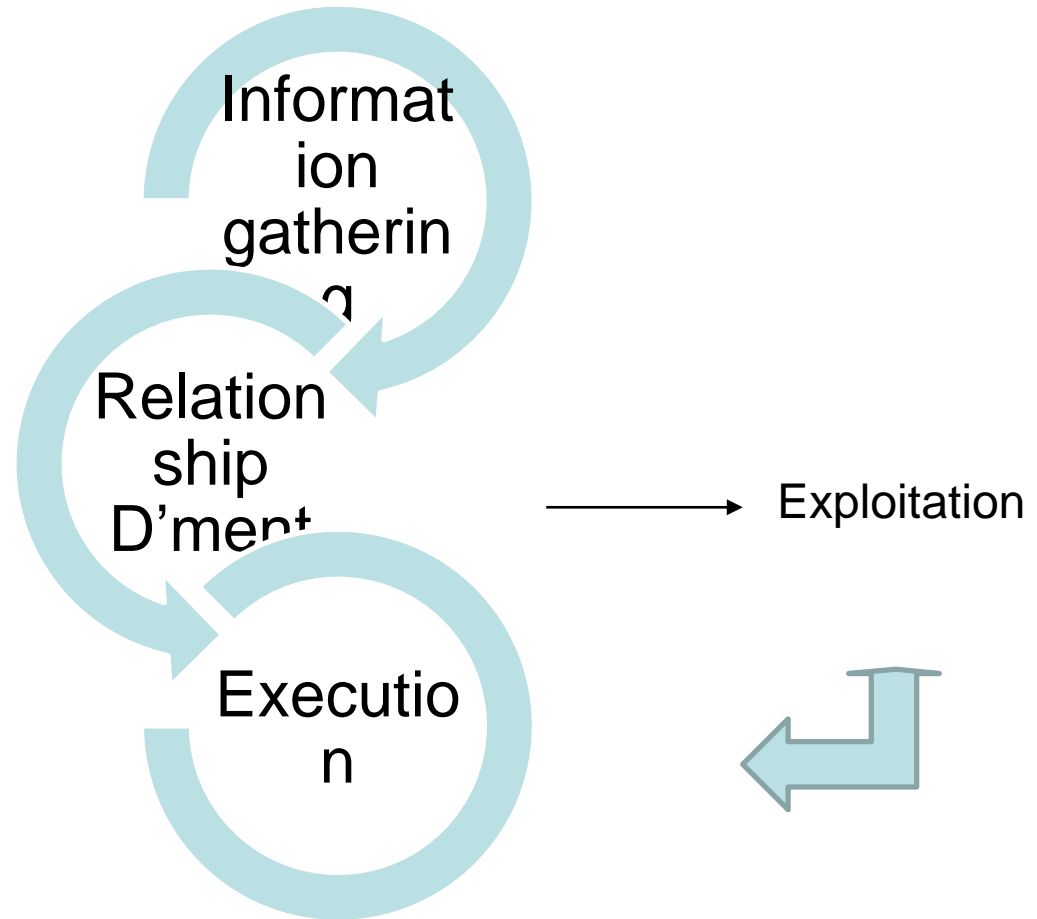


- Any act that influences a person to take an action that may not be in their best interest.
- Human hacking has been identified by Interpol as one of the world's emerging fraud trends.

What does it mean for children?

- If Humans for that matter children are the weakest link in the security chain.....
- Predators find it easier to exploit the vulnerabilities in the systems & children.
- Picking devices for children either for many reasons but failing to equip them about the responsible use.

The 4 stage of scam



How to spot Social engineering

- Unusual requirements.
- Requiring respect for authority.
- Threatening with negative consequences.
- Giving praises and flattery.
- Offering something for nothing.
- Seems too good to be true.



How can we ensure an effective Child Protection System online in Africa?

Please list your response in the order of priority.

1. Political will or Commitment
2. Funding
3. Education and awareness
4. Channel for reporting
5. Digital literacy and skills.
6. Coordination among stakeholders
7. Research

The Child Online Protection Initiative

Objectives

VISION: “We are creating a world where children can be connected and are able to fully benefit from the opportunities of a trusted and safe online environment”.

- 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 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.

10 years after their first publication, been re-thought and re-written by a multi-stakeholder expert working-group. Taking inconsideration the special situation of children with disabilities and issues around new technological developments.

A local policing mechanism required by each country to promote safety of children and young people who are making use of the Internet.

One of the new twist to the COP Initiative this year is the introduction of a Mascot.



The 5 strategic pillars to implement the guidelines are based on:

Legal Measures: A strong and comprehensive child protection legislative framework in place at national level to address issues of Internet safety.

2. **Technical and Procedural Measures:** The fact that children and young people are communicating using several platforms, their protection is made paramount by default. It also means proactiveness on the part of providers.

3. **Organizational Structures:** Good organizational structures need to be in place at national level to facilitate the infrastructure for safe and trustworthy digital space.

4. **Capacity building:** An effective awareness raising strategy has to be in place at national taking into consideration a country's peculiar needs.

5. **International cooperation:** The Internet know no boundaries, this COP initiative takes into concedes that online child abuse is a global c that requires international collaboration.



What do we hope to see?

- Promote the culture of safety & protection for children.
- Perform periodic performance audits.
- Train stakeholders to recognize & resist attacks/threats.
- Follow policies & procedures.
- Reporting channels or portals.



The status of children online.



COP guidelines for Policy Makers

ITU Publications

International Telecommunication Union
Development sector

Guidelines for policy-makers on Child Online Protection 2020



Risks & Harms online

According to recent research by Broadband Commission:



- In 2018, the US National Center for Missing & Exploited Children (NCMEC) received 18.4 million reports of (CSAM) online.
- A recent study found that 17% of parents said their children had been a victim of cyberbullying. Some countries, that figure was as high as 37%.
- According to the 2017 DQ Impact Report, 56% of 8-12yo across 29 countries have at least one cyber-risk on average: including cyberbullying, video-game addiction, sexual behaviors, and offline meetings.
- 1 in 5 children aged between 9 and 17 see unwanted sexual material online and 25% of them reported experiencing extreme fear or distress.
- A 2019 study found that 99% of online terms and conditions were written in language too complex for children to understand.
- The number of illegal images and videos confirmed by INHOPE's Internet Hotlines increased by 83% from 2016 to 2018.
- INHOPE also reported that the prevalence of pre-pubescent children (3-13yo) depicted in CSEA images and videos increased from 56% of all illegal material (122,276) in 2016, to 79% (148,041) in 2017 and 89% (223,999) in 2018.

A digitized society should prioritize COP.

BEST PRACTICE

1. Creating a single authority with ultimate responsibility for COP in country.
2. A robust legislative regime in place for prosecution and all.
3. Ensuring products and services are safe by design and by default.
4. Build a connected ecosystem in which :prevention, detection and intervention work seamlessly together.
5. Coordination with different agencies at the national and regional level. Thus: Government entities, Private sector, Civil Society and Research institutions.
6. Educating children, parents and caregivers on their rights and ensuring they know who/where to turn to if they need help.

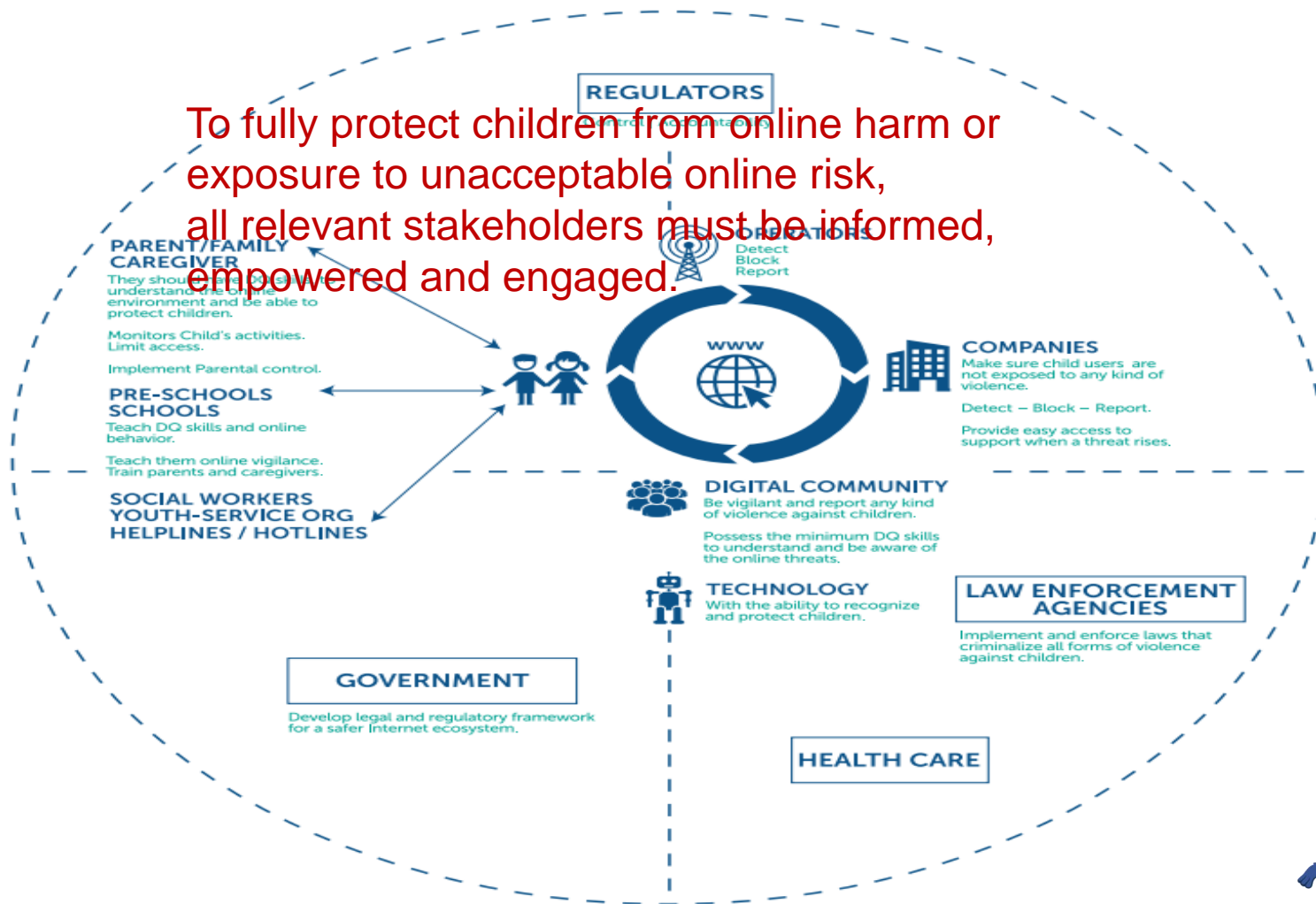


COS Universal declaration:

What SAFER means to a child.

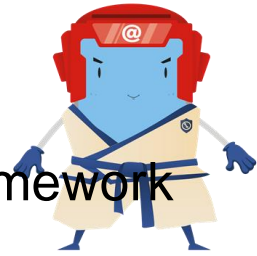
Safer Internet Ecosystem

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



What the child needs

UNCRC.ACERWC.AGENDA2030 & AGENDA2040

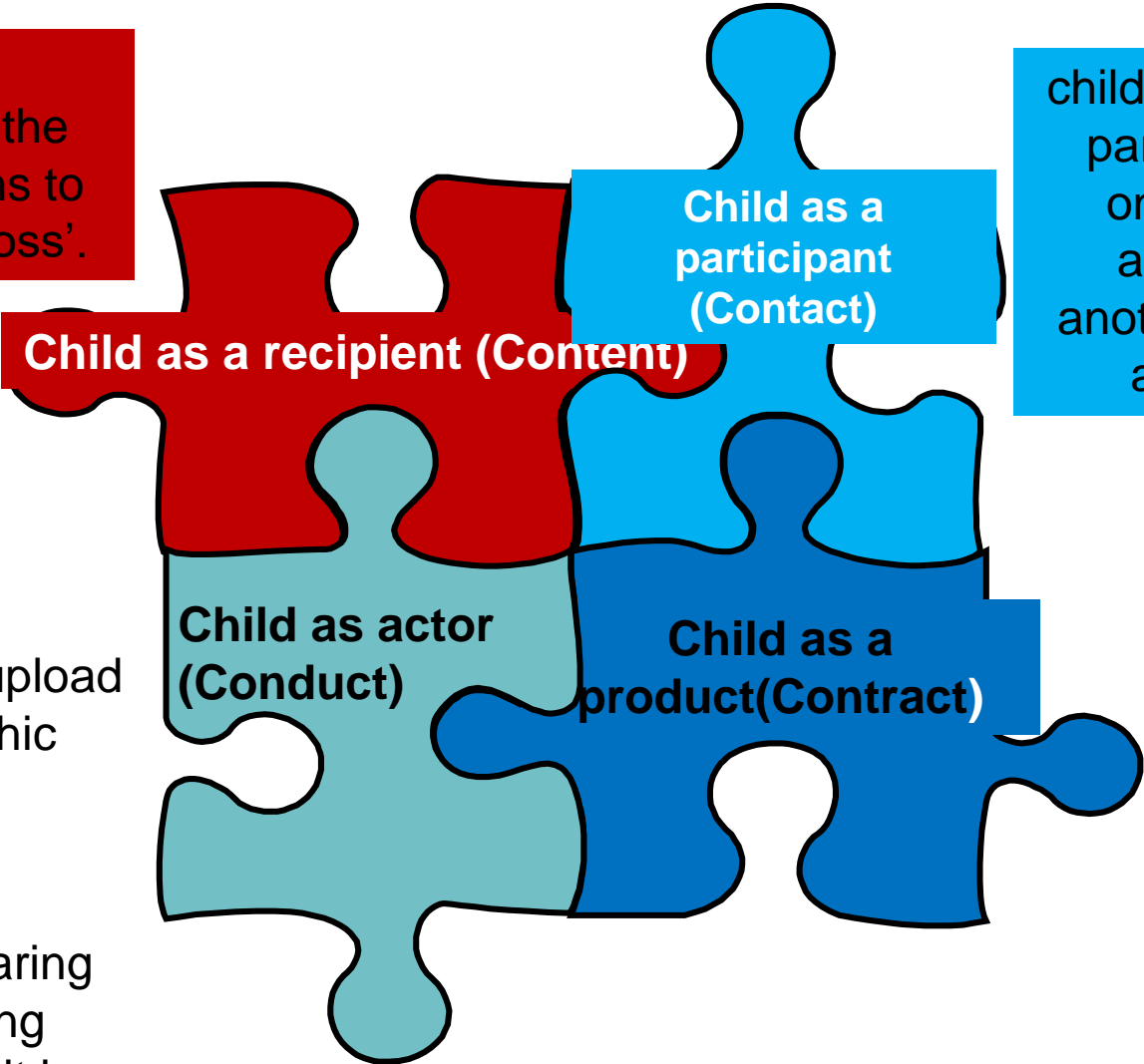


- Be protected by a robust, effective, and enforced legal framework that promotes children's rights. (Protection)
- Use child-appropriate online solutions and services that were designed to protect children and mitigate risks. (Provision)
- Be empowered by a set of comprehensive digital competencies that can enable children to minimize risks and maximize potentials on the Internet; recognize when their rights are being violated; and be supported by adults who understand children's rights and how to safeguard them online, who have access to safe and trusted mechanisms to report any violations of those rights. (Participation)

Risks categorization for children online



General information the child happens to 'stumble across'.



child targeted as participant in one-to-one activity by another child or an adult.

create or upload pornographic material, bullying or harassing others, sharing PII, friending strangers, it is

Data collected without consent, sold & re-sold. Unclear T&C, etc

Cont'

Table 3: A classification of online risks to children

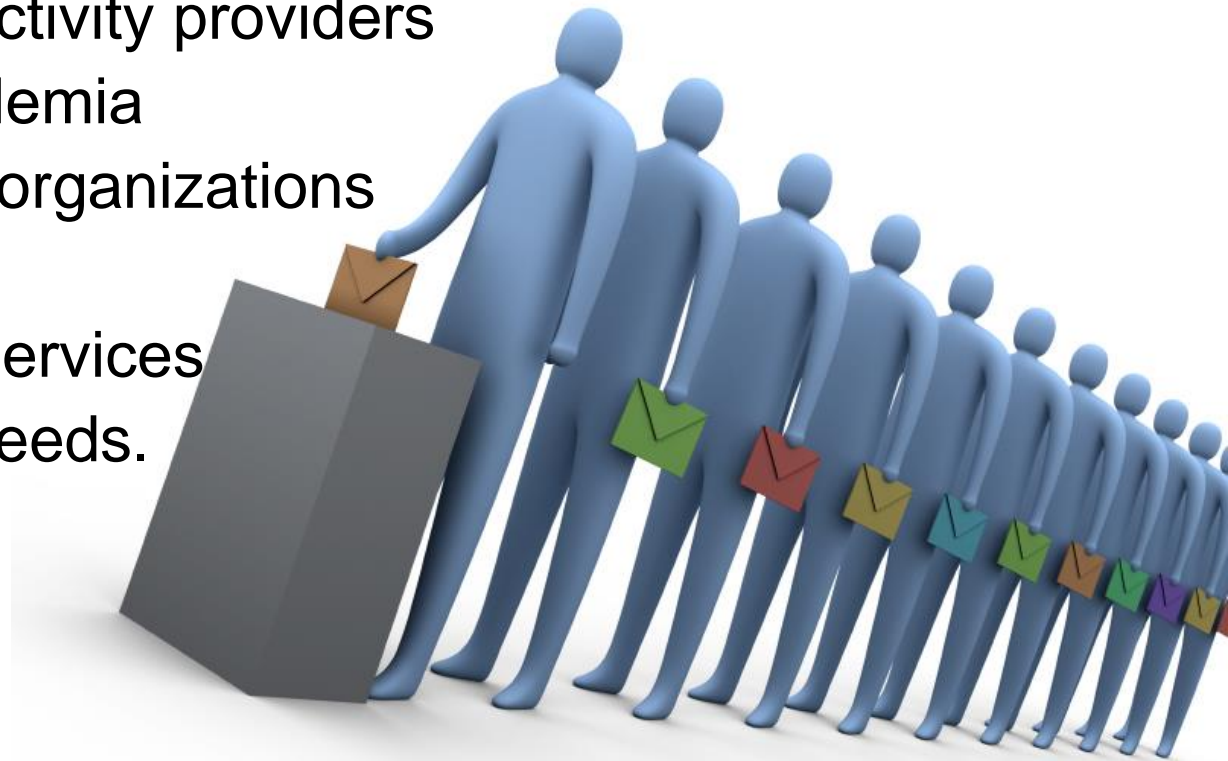
	Content Child as receiver (of mass productions)	Contact Child as participant (adult-initiated activity)	Conduct Child as actor (perpetrator / victim)
Aggressive	Violent / gory content	Harassment, stalking	Bullying, hostile peer activity
Sexual	Pornographic content	'Grooming', sexual abuse on meeting strangers	Sexual harassment, 'sexting'
Values	Racist / hateful content	Ideological persuasion	Potentially harmful user-generated content
Commercial	Advertising, embedded marketing	Personal data exploitation and misuse	Gambling, copyright infringement

Source: EU Kids Online (Livingstone, Haddon, Görzig, & Ólafsson, 2010)

Key stakeholders for COP



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



A policy guide to deliver trustworthy COP



The policy makers guidelines take into account the ff :

- Introduction to the risk and threats to children online.
- Preparing for a national Child Online Protection strategy.
- Recommendations for framework and implementation.
- Developing a national Child Online Protection strategy.

All these topics with sub-topics and examples aimed at providing an idea of what countries should consider in getting it right with Child Online Protection Initiative at the national and local levels.

Online with

AfriKavi

Legal framework

Educ. digital literacy & competency

Regulatory framework

Educational resources

Reporting illegal-content

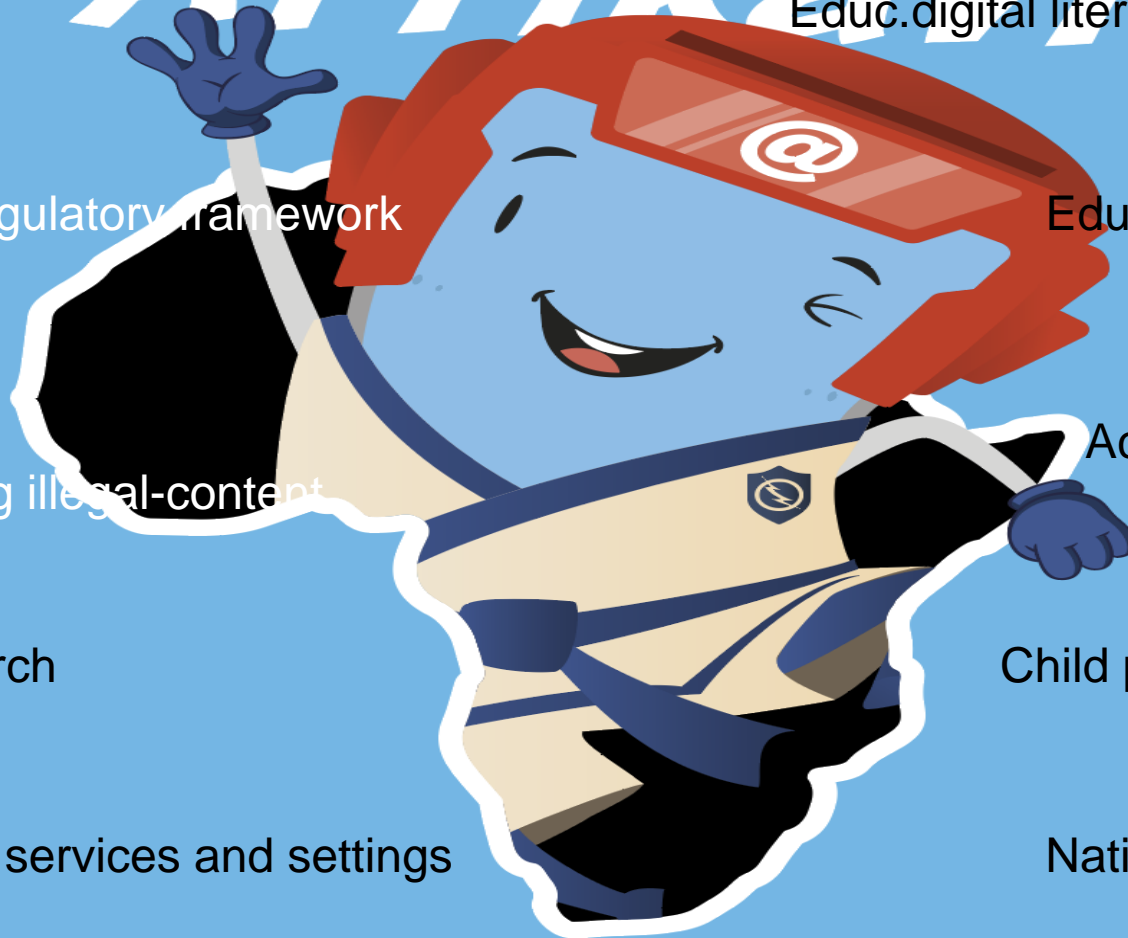
Actors & stakeholders

Research

Child protection

Tools, services and settings

National awareness





Thanks for your attention

