Report of the ITU Annual Capacity building workshop on Child online safety for African countries

Lilongwe –Malawi 18-20 July 2016

The ITU annual regional human capacity building workshop for African countries on Child online protection on the theme **"Ensuring child online safety (COS) in a digital world: building human capacity in COS policy formulation and implementation"** was held in Lilongwe in Malawi from 18 to 20 July 2016. This regional workshop was organized by International Telecommunication Union (ITU) in collaboration with the Common Market for East and Southern Africa (COMESA) and the Malawi Communications Regulatory Authority (MACRA) host of the event.

This regional capacity building workshop was a follow up of the First African Child online Conference (ACOP) held in 2014 in Uganda.

The opening remarks were delivered by Hon. Patricia Kaliati , MP, Minister of ICT and civic education of Malawi for the opening ceremony and the opening remarks of the parents, educators and children interactive sessions were delivered by the Principal Secretary of the Ministry of Gender, Children, Disability and Social Welfare, Dr. Mary Shaba.

The objective of this workshop was to provide a platform to African countries to share experiences, strengthen their knowledge and raise awareness on children and youth safe digital inclusion through a multi-stakeholders approach involving the role of educators, ICT/telecoms regulators and ministries, industry civil society, NGO and other organizations dealing with children and youth.

This workshop also helped participants to further understand framework, tools and guidelines already developed on child online protection and available by ITU and its COP partners, to assist them in developing, adapting and implementing national strategies, thus contributing to Sustainable Development Goals (SDG) in achieving social economic development through the use of telecommunications/ICT.

It also presented real case studies of countries with successful COP model structure and highlighted the importance of national, regional and international cooperation, the importance of Public and Private Partnership (PPP)/collaboration on Child online safety. Practical training sessions on child online protection and live interactions were held.

This workshop was attended by more than 115 participants from 17 African countries, regional and international organizations, industry and private sectors as well as national countries stakeholders from Malawi.

This workshop discussed about different aspects related to children online safety and digital empowerment. The sessions of this workshop are presented as follow:

COP in Africa: Institutional framework: Policy and regulation

- During this session ITU made two presentations to shade light on the COP initiative, COP platform and working group , ITU activities undergoing such as assisting countries to develop their national strategy on child online protection, statistics on country COP profile wellness in Africa, as well as presenting the Connect 2020 agenda for telecommunication/ICT development. The role and importance of international cooperation, partnership between multi-stakeholders was also highlighted to mitigate risk and raise awareness on children safety and build human and institutional capacity building of their stakeholders to efficiently address COP.

An in-depth presentation of the COP guidelines for policy makers was also made to enable participants understand how to formulate a national strategy by defining a clear legal framework, by involving all stakeholders having an interest with children online safety. It was further emphasized that education and awareness were essential when formulating a national strategy and that not only a reporting mechanism should be established and widely promoted but also there is a need to have law enforcement resources available.

- **ECPAT** also made a presentation on child online abuse and exploitation, the global threat and response related to child online safety. This presentation help the participants to understand the various aspects of sexual exploitation conducted online and their evolution such as sexting, sexual grooming, child sexual abuse image or live streaming of child abuse affecting both connected and non-connected children. The drivers of child sexual exploitation were explained. In addition, the trend and profile of the victims were shown as well as the different human rights obligations and also emphasized on AU convention on cybersecurity and personal data. A national model response framework developed by "WeProtect" to prevent and tackle the child sexual abuse and exploitation developed around the following key areas was also presented: policy& governance, criminal justice, victim, societal, industry and media/communications. They also presented a short video to demonstrate on key aspects revolving the topic.

- **MACRA** also made a presentation on the child online policy and framework of Malawi focusing on the current status of COP in Malawi, the development of a national cybersecurity strategy with a need to integrate the specific aspects related to child online protection, different challenges being faced but also initiatives undertaken by the government to tackle the children online safety

The following concerns were raised by participants and addressed by speakers:
- ➤ Raising awareness on child online protection instead of mitigating risk can sometimes become a provoking factor and increase numbers of offences or abuse against children as we see in other areas such as end of female genital mutilation or albinos killing
- ➤ Radicalization of children online is being neglected while tackling issues to do with COP
- ➤ Link between tools developed on COP and the country approach
- ➤ Initiatives such as COP special day should be in place to promote and raise awareness on children safety by ITU
- ➤ Are there in ITU any Strategies, approach or Framework for monitoring, measuring COP activities to share with countries developing their national strategies
- ➤ Access to cyber-cafes in local communities should be regulated and websites filtered to limit predator's activities within these facilities.

Industry: Technical measures taken by the industry to mitigate online risks and access to online abuse content/services

- ITU gave an overview on the new COP guidelines developed for the industry to help participants understand the technical tools that can be locally adapted and domesticated by various industry players in their countries but also briefly introduced them to the online platform case studies of some big industry players like the Mobile Network Operators (MNO's), Internet Service Providers (ISP's), broadcasters, content providers, social media service providers, hardware manufacturers.

- GSMA made a presentation on "Notice and Take down" of child abuse material to help combat access to child sexual abuse content through their network/services. This presentation explored the toolkit that the Mobile Alliance has developed in collaboration with UNICEF to help the ICT providers community prevent the misuse of their services by sharing child sexual abuse material and to rapidly deal with such content in a manner which prevents re-victimization of children but also correctly manages potential evidence for use in rescuing children from abusive situations.

- Facebook gave an overview of its mission, which is to give people the power to share and to make the world more open and connected. They stated that creating a welcoming and safe platform for everyone is core to their mission. Facebook wants people to feel safe using their platform, which is why Facebook has created a set of policies, which set out what is and is not okay to share on Facebook – their Community Standards. They also noted that they have created a number of tools and resources to give people control over their experience, which people can use and access for free, such as reporting, blocking, and regular privacy and security checkups. Facebook also stated that it focuses heavily on keeping teens safe, has zero tolerance towards child exploitation imagery and takes proactive measures to protect young users from predators, including using technology known as PhotoDNA to block the sharing of CEI and report this content to the National Center for Missing and Exploited Children, which works with law enforcement agencies around the world. Facebook reviewed its Community Standards and encouraged everyone to report content of concern directly to Facebook as there is general underreporting taking place in Sub-Saharan Africa. Lastly, Facebook emphasized the need and interest in entering into more partnerships with NGOs and civil society groups to educate young users, parents and teachers on the importance of staying safe online and the resources that are available. They pointed to an international multistakeholder effort to thwart the proliferation of child exploitation known as WePROTECT, on which they serve on the Board, as a good example of how to collaborate on these important issues and as a resource for countries looking to address the issue of CEI

  Concerns raised and addressed
  - Visibility of safety information on Facebook platform and how to find the safety resources online
  - Providing free training materials to educators on COP by industry players
  - Revictimization: what can be done to avoid re-abuse of children online by posting same content online after take down and notice
  - Is Facebook giving access data to their databases to organizations/government on request
  - How can GSMA ensure that all industry players apply the same code of conduct/policies in Africa as they do in other countries
  - Is there any software available to block nude images/pictures
  - How do you ensure that there is proactive enforcement of regulations for operators that takes into account of COP initiatives?

Organizational Structure: successful country COP model

- **Egypt:** The presentation of Egypt was focused on the multistakeholder approach model set up in the country with a committee involving all national stakeholders and industry players dealing with children under the leadership of the Government. They also explained how in Egypt COP is integrated in the formal education curricula but also how some non-formal education activities

are undertaken such as competitions, games or parents training are undertaken all over the country to raise awareness. They also showcased children activities on COP and awareness sessions as well as played a video on safety campaign made by the committee.

- **Mauritius:** CERT Mauritius also gave an insight of the CERT-MU structure and services provided in general within the country and but also presented the child online safety action plan being implemented by CERT-MU which includes multiple stakeholders in the country and which comprise of 24 projects. CERT-MU is responsible for carrying out awareness campaigns throughout the country for students, teachers (train the trainer) and parents. Incidents such as online harassment, Identity Theft, Hacking, Inappropriate content related to Child Online Safety are reported to CERT-MU and the victims are given appropriate assistance. They also explained that in Mauritius, the School net project is operated by the Data Center (Government Online Center) of the Government whereby inappropriate/harmful online content is filtered for the schools and colleges connected to the internet. The Information Communication Technology Authority (ICTA) has put in place a child sexual abuse content filtering system to mitigate the risks of access to such content in Mauritius and the presentation included the network diagram of this system. During the presentation, a video was played to portrait the evolution of the online world with regards to Children's Safety

- **Uganda:** In their presentation, they gave an overview of the statistics on child online safety in 2015.In addition, they also introduced a handbook of the directorate of Public prosecution as well as Tracking, Referral and Response (RTRR) Guidelines on violence against Children in Schools. They also highlighted on the reporting mechanism put in place through collaboration and partnership with International organization and briefly presented the national cybersecurity strategy.

- **Cameroon:** The presentation made by Cameroon showed the activities and role of ARTAC within the region. An overview of the status of child online protection was provided covering key aspects like legislative framework. Finally, some observations and proposals were made to ensure children safety.

- **Zambia:** The presentation made by Zambia focused on the country profile, ICT sector profile, statistics of a survey conducted in 2013 and 2015 to assess online risks and prevalence of illicit content among internet users in Zambia. They also shade light on COP initiatives and framework within the country. In wrapping up, steps undertaken to move forward when addressing child online safety were also pointed out.

- **Kenya:** Kenya presented the country data profile on ICT but also statistics on youth aged between 12 and 17 in respect to use of Internet and preferred devices used to access the Internet. An overview of past COP initiatives and activities were presented as well future activities and action plan on campaign in 3 phases targeting parents/guardians, children and policy makers. Phase I of this campaign has already been launched in Kenya. They also highlighted the importance of public private partnership as well as collaboration to ensure children online safety involving all stakeholders. Phase II will also take into account COP guidelines to facilitate developing a national strategy for Kenya.

- **Namibia:**Namibia presented the current status of child online safety in the country and framework put in place,the stakeholders involved on COP, showed jingle of the awareness campaign and further shared some statistics on studies and research done on knowledge, attitudes, and practices of ICT use and online protection risks by adolescents (between 13 and 17 of age)

  Concerns raised and addressed
  - ➢ Kids engaged in the discussion in countries before developing policies related to COP

- ➢ Difficulties/challenges faced when it comes to funding COP activities or national committees set up in a country
- ➢ Who should take the lead in a country for a COP strategy development
- ➢ Occurrence of national Committee meetings scheduled

COP training on children and technology

Children and young people are among the most avid users of internet and mobile technologies and this can bring, a tremendous positive impact on their lives. Like any other tool, , internet and mobile technologies can be used to cause harm In view of this development, parents, caregivers, governments and industry have a crucial role in protecting and supporting children who are connected. This training looks at the issue from several angles, including ITU-UNICEF Guidelines for Industry on Child Online Protection, the main risks and combinatorial approach to the issues

Education and awareness

- **UTTA Malawi on Girls in ICT and tennis:** This NGO demonstrated how they are combining sport and ICT by training girls in the use of ICT programs (i.e. MSOffice: Excel, PowerPoint presentation) but also conducting training on girls online safety such as awareness of trafficking, use of restrictions techniques on social media platform after their tennis schedule regular training .They also encourage the girls by giving them during tennis tournament prizes related to ICT devices or education when they win. They however emphasized also on the financial and material challenges they are facing in Malawi to support their activities.
- **Watoto Watch Network Kenya child online protection program :**This local NGO mainly focused on COP and made a presentation on their activities in raising awareness through educative campaigns and training program all over the country targeting parents, children, educators, law enforcement and other stakeholders. They also showcased some video materials and presentation used for conducting training on COP and translated in Swahili.

- **ISOC Uganda Chapter: T**he presentation gave an overview of ISOC work undertaken in Uganda as well as activities such as research and studies on Internet online safety, educative training programs and sensitization campaigns on COP and safety toolkit developed.

    ### Concerns raised and addressed
    - How to ensure that the girls in sport are protected in an dominant male environment during trainings sessions
    - What reporting mechanisms do you have in place that encourage young girls to be open and free to report abuse or any traces of it?

Interactive sessions with kids/parents and educators from Malawi

Two parallel interactives sessions were conducted with children on one side and the parents/teachers on the other side to capture Children activities on the Internet, knowledge of Risks online and advice on how to stay safe online.

1. **Children interactive session: 50 children from secondary schools in Lilongwe aged between 13 and 17 were invited to this session**

It was an interactive Q&A session during which 3 videos on grooming, sexting and cyberbullying were shown as well as a practical session on reporting mechanisms on social media platform based on children choice: FACEBOOK and WhatsApp.

Questions raised by young people

- How do we deal with hackers from other countries?
- How do I handle someone who has posted a nude photo of another friend of mine on their social network page?
- Who do they report to if they are cyber bullied?

Observations on children Internet safety awareness and usage

- Majority of children use the Internet for chatting via social networks
- Children were not aware of any legal repercussions in case of abuse on the Internet or misuse of ICT services
- Majority of them would not report on their friend's bad behavior, usage of inappropriate images/content or activities online to the police or teachers. They turn to their peers for support.
- No understanding on reporting process on social media platform

Recommendation of moderators of this session based on the outcomes of this training session

- Targeted awareness activities of children in schools.
- Reporting options in the country on ground/police.

2. **Parents and educators interactive sessions: 10 parents and teachers from Malawi were invited to take part in this session**
A short video was played on a grooming case scenario of a sexual predator of a young girl as part of a brief training of parents/educators on children online risks in the cyberspace. The moderators then gathered the feedback and comments from parents/educators on "**what they have observed**", and is presented as followed:

Observations

- Communication breakdown between children and their parents
- The child has her own computer in an environment (bedroom) that is not monitored
- The child gives out critical information with ease because of the trust she builds on the predator online
- The predator increased the child's level of confidence through conversations
- The predator lure the child by faking his age and engaging her as if they are of the same age
- There was no supervision on what the child was doing online; she conversed in a secluded room and switches off the monitor of her computer when going out of the room to conceal her dealings.
- A child is defenseless when he/she is left in solitary and is presented with unguided use ICT in front of them which may lead to abuse of the technology.

Parents and educator on recommendations to help children safety

- Parents must not leave kids with technologies devices without monitoring them and also must engage a dialogue with their kids on ICT advantages and risks.
- Parental control tools must be used on device that kids have access to,with the aim of mitigating online risks
- Integrate in the education curricula, modules on the safe use of ICT by children or allow some local NGO to conduct trainings in schools or public places to help disseminate the information and raise awareness on child online safety and protection
- Parents should teach their own children not to trust any stranger online
- Use of SMS to send out to the community ICT safety messages
- Have a database and share information on sexual predators
- Need to train kids-Parents-educators on how children can remain safe online and strengthen their knowledge on the use of ICT.
- Conduct awareness campaign and training for non ICT users
- Countries should filter access to child sexual abuse content
- National Internet governance forum to be enhanced or strengthened
- COP discussion should be part of agenda of ICT regional ministerial meetings to engage government and decision makers at a higher level to take the lead on child online safety in Africa
- Parents should also bear in mind that some threats may be nearer to children through relatives and close friends more especially in Africa where we have extended family relatives living in our homes
- Parents should move to social media befriend their own children for easy monitoring but do not be intrusive.
- Industry should do more research on how gadgets that can particularly be designed for children can be used as tools for monitoring their activities at the same time striking a balance between monitoring and privacy

The session was concluded by a short presentation of ITU on COP guidelines for parents-educators to help them better understand how they can keep their children safe in the digital world. Tips and advises from the COP guidelines for children as part of the "BE SMART BE SAFE" campaign was also presented for children responsible use of ICT and Internet services by children

Children Data Protection and Security in the cyberspace

- **ICANN**: The presentation focused on ICANN key areas of operation (capacity building, analytics, Threats awareness and preparedness, trust-based collaboration) and importance of collaboration between the cybersecurity and safety community and ICANN response team to identify and mitigate risks as well as information sharing related to identifier system misuse.
- **Commission of Information and Liberties (CIL) BurkinaFaso:** The presentation mainly focused on the problems related to personal data protection in the cyberspace as well as key elements and challenges to secure information systems.
- **CERT-**Mauritius: The presentation was an insight on type data threats, showed some statistics and recent incidents that have recently occurred in the cyberspace and finally presented CERT-MU cybersecurity strategy for data protection.

Concerns raised and addressed

- Steps taken in Burkina Faso to ensure children safety in the cyberspace
- Content deletion procedures and responsibility. Collaboration between police and investigation unit prior to content deletion.
- Dark web handling and issues
- Drone utilization and impact on countries national security
- IP address management process by ICANN, Legal status of ICANN and importance of information provided by ICANN to Law Enforcement Agencies (LEA)
- Fake account/domain management and mechanisms in place to track down perpetrators to mitigate children online risks
- Takedown requests processing and who finally deletes offending domains / content?
- Technical tools to prevent/limit children access to certain content
- Difficulty of Internet governance and perceived overlapping interests between ITU and ICANN by the ordinary public.
- Global legislation to address Child Abuse Material or pornography
- How do we deal with 'dark web' that is being used to further perpetrate child online abuse?

Multi-stakeholders panel discuss on COP

This session discussed about the way forward for each stakeholders perspective and allowed the meeting to make the following recommendations to tackle children online safety and security taking into account all aspects intensively discussed during these 3 days.

1. **All African countries should formulate their national framework and start the dialogue involving all stakeholders a national level within next 3 months after this capacity building workshop on COP to permit regional harmonization of frameworks on COP**

2. **Include COP on the ICT regional ministerial meetings agenda to engage government and decision makers at a higher level to take the lead on child online safety in Africa**

3. **Continue to Promote ratification of African Union cyber security and personal data protection convention by African countries**

4. **Encourage countries to engage all stakeholders/key industry players before formulating national COP strategy and to integrate the awareness programs for Children who are not connected and their access to new technologies or Internet when developing their national strategies**

5. **Encourage countries Identify children trainers at national level as well as having and promoting children ambassadors on COP to efficiently promote and raise awareness on COP**

6. **Regional guidelines for Africa on COP on best practices, legal frameworks, codes of practices for industry players to be championed by ITU/ATU and different sub regional organizations.**

7. **ITU should help develop train the trainers programs for countries in respect of all relevant stakeholders (legal, judiciary, educators/parents, children, etc.…)**

8. **ATU/ITU to set up specific platform for Africa and also set up an African working group/task force on COP from international, regional organization, industry players, NGO**

to share experiences, trainings materials , organize workshop, common activities among others

9. ITU should promote COP awareness and activities during ''Safe Internet Day 'celebration all around the world

10. Encourage countries to identify specific department/agency to handle cyber security issues and threats and to set up a national COP committee on COP to coordinate/manage all COP activities.

11. Encourage countries African countries should have a strategy/framework that focuses on the following pillars, including but limited to:

    A.   Awareness Raising for all target/concerned audience

    B.   Technology Solutions

    C.   Laws and Legislations

    D.   Media

    E.   Education and Capacity Building

    F.   Research and Studies

    G.   International Cooperation