



Statement by KICTANet during the Third Substantive Session of the Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies
2021-2025, UN Headquarters, New York
27 July 2022

Grace Githaiga, Convenor, KICTANet
www.kictanet.or.ke

Mr. Chair,

The Kenya ICT Action Network (KICTANet) is a multistakeholder platform and think tank established in 2005 and is based in Nairobi. The network provides mechanisms and a framework for continuing cooperation and collaboration in ICT matters among stakeholders. It also encourages synergies for ICT policy-related activities and initiatives through advocacy, capacity building, research, and multistakeholder engagement.

We would like to thank the Chair and all Member States for their work in advancing the mandate of the OEWG and welcome the various proposals made on the topics discussed during this third session. In particular, we welcome the measures directed at addressing the specific capacity building needs of developing countries; tackling the gender digital divide; promoting confidence building measures; enhancing regular institutional dialogue; and recognising the roles of regional and sub-regional institutions.

More importantly, we welcome the mechanism put in place by the OEWG to promote engagement and interaction between stakeholders and government delegations, and encourage Member States to implement similar engagement at the national level.

In response to the questions provided by the Chair, we would like to respond to the first set of questions as follows:

1. What are the various ways in which stakeholders are currently involved in supporting and/or delivering capacity-building initiatives in the context of the current ICT security capacity-building landscape?

KICTANet has and continues to:

- Conduct research on existing and potential cybersecurity threats and risks; policy and legislative developments; the impact of emerging technologies; and makes proposals for reform of policy, legislative and institutional mechanisms.
- Create awareness on cyber hygiene, digital security, and provide digital resilience support to civil society organisations.

- Promote multistakeholder engagement at the local and regional level. For example, KICTANet convenes regular topical thought leadership forums and the [Kenya Internet Governance Forum \(KIGF\)](#) which this year, was held in June and attended by 500 people.
- Advocate for greater cooperation and information sharing among stakeholders, and for the implementation of human-centric approaches to cybersecurity. KICTANet has been part of a group of regional stakeholders who, during the African School on Internet Governance, identified various capacity building needs and will share our concrete proposals from the engagement.
- Development of curricula on cybersecurity and cyber hygiene targeting the digitally marginalised and excluded populations and vulnerable groups such as children, women, farmers, and persons living with disabilities. For example, KICTANet hosts the annual Kenya School of Internet Governance (KESIG) which has so far trained 500 students since 2016 on internet governance. KICTANet is also contributing to the development of a cybersecurity curriculum by the Global Forum on Cyber Expertise (GFCE).

2. What kind of capacity-building initiatives or projects can stakeholders most meaningfully and effectively contribute to? Are there certain types of initiatives (e.g. technical training, skills training etc.) that present particularly suitable opportunities for meaningful and effective contributions from stakeholders?

Civil society can contribute by:

- Conducting capacity building in the use of ICTs such as by offering digital safety and security training and cyber hygiene awareness programmes for the public.
 - Providing technical support to enhance the digital resilience of civil society organisations.
 - Conducting evidence-based research on emerging cybersecurity issues of concern; conducting assessments, and reviewing the implementation of confidence building measures, and the implementation of rules, norms, and principles of responsible state behaviour in the use of ICTs.
 - Promoting awareness at national, regional, and international level of cybersecurity as societal security, including through the development of knowledge products and tools to promote digital literacy, resilience and awareness.
 - Contributing to the development and implementation of comprehensive national cybersecurity policies, strategies, standards, and legislation.
 - Participating in and convening regular multistakeholder engagements at national and regional level as platforms for institutional dialogue, building trust, enhancing coordination and sharing information and best practice.
- 3. What forms of stakeholder involvement (e.g. contribution of technical resources, co-creation of programmes, contribution of time and expertise of skilled individuals) work well and what forms of stakeholder involvement work less well?**

- Contributing technical and knowledge resources, including by providing specialised expertise in the development of cyber policies, legislation and strategies.
- Co-creating capacity building programmes for key stakeholders in the relevant thematic areas.
- Hosting focused discussions and participating in regular dialogue to enhance coordination and to exchange information, knowledge and best practices.
- Collaborating in the conduct of evidence-based research to inform policy-making and contribute towards the assessment, monitoring and evaluation of the impact of various cyber security initiatives and the implementation of measures.

What has not worked well are cyber processes that are not open, inclusive and multistakeholder in nature, whether at national, regional and international level. While stakeholders such as civil society organisations from the Global South do not have significant financial resources, they remain ready and willing to meaningfully engage and effectively participate in key processes, and implement targeted programmes.

Finally Mr. Chair, we encourage the implementation of capacity building initiatives by Member States and other stakeholders. We also call for financial support to Global South civil society to enable them to effectively contribute to the OEWG and deliver useful outcomes in their regions.

/Ends