# ENABLING CYBER DEFENCE IN AFRICA THROUGH STANDARDIZATION

Mwende Njiraini, Chair SG17RG-AFR, Communications Authority of Kenya; Racky Seye, Vice Chair SG17RG-AFR, Ministère de l'Economie Numérique et des Télécommunications
Senegal

## 1. EXTENDED ABSTRACT

Cybersecurity has implications on the social economic development with increased use of technology in education, agriculture, health [1]. With persistent virtual realities accelerated by the COVID-19 pandemic, it is imperative that African countries build capacity and effectiveness in cybersecurity through the implementation of relevant ITU-T Recommendations and supplements [2].

ITU-T Recommendation X.1060: Framework for the creation and operation of a cyber defence centre, defines cyber defence centre (CDC) as an entity that plays a central role in an organization to address cybersecurity risks. The framework describes the build, management and evaluation processes that a CDC should implement as well as services that the organization should have in order to implement specific cybersecurity measures.

A survey of CDCs in Africa has been proposed for January 2022 as the first step towards implementation of X.1060 [3] with the possibility of extension to other ITU Member States in the future. The survey is intended to disseminate information on security standards and standardization, support the operationalization of cyber defence services and initiate collaboration, pursuant to provisions of ITU Resolutions [2, 4, 5, 6].

The <3 minute video starts by explaining Africa's commitment to cybersecurity and capacity for response to threat remain low compared to other continents despite increased connectedness of the physical and virtual worlds [7]. The video provides an overview ITU-T Recommendation X.1060, the progress that the ITU-T SG17 regional group for Africa has made in implementing X.1060, and how that will improve cybersafety.

## REFERENCES

[1] D.K. Sparrell, "Cyber-safety in healthcare IoT", Proceedings of ITU Kaleidoscope 2019: ICT for Health: Networks, standards and innovation; pp 163-179.

[2] World Telecommunications Standardization Assembly Resolution 50, *Cybersecurity*, 3-Nov-2016, available from https://www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.50-2016-PDF-E.pdf.

[3] Recommendation X.1060 (2021), *Framework for the creation and operation of a cyber defence centre,* ITU Telecommunications Standardization Sector (ITU-T).

[4] World Telecommunications Standardization Assembly Resolution 54, *on Creation of, and assistance to, regional groups,* 3-Nov-2016, available from https://www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.54-2016-PDF-E.pdf.

[5] World Telecommunications Standardization Assembly Resolution 44, *on Bridging the Standardization Gap*, 3-Nov-2016, available from https://www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.44-2016-PDF-E.pdf.

[6] World Telecommunications Standardization Assembly Resolution 58, *Encouraging the creation of national computer incident response teams, particularly for developing countries*, 3-Nov-2016, available from https://www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.58-2016-PDF-E.pdf.

[7] International Telecommunications Union, *Global Cybersecurity Index*, https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx