Doc No. 25/EACO/G/1/2023

EACO East African Communications Organisation

Communications for all in East Africa

GUIDELINES FOR THE MANAGEMENT OF CRITICAL INFRASTRUCTURE

Prepared by EACO

JUNE 2023

TABLE OF CONTENTS

DEFINITION

Critical Infrastructure means vital virtual systems and assets whose incapacity or destruction would have a debilitating impact on the security, economy, public health and safety of the country.

ACRONYMS

CERTS	Computer Emergency Respond Teams
DNS	Domain Naming System
GCCN	Global Crisis Centre Network
HLRs	Home Location Register
ISPs	Internet Service Providers
IXP	Internet Exchange Point
NOFBI	National Optic Fiber Backbone Infrastructure

1.0 Background

Under the East African Communications Organisation (EACO) strategic plan of 2018-2023 it was identified that Communications infrastructure is very important taking into account the huge investment and the impact it has on security, governance, social and economic wellbeing of the society.

Considering the importance of this infrastructure, it was considered as critical and therefore calling for protection and proper management for ensuring constant service availability.

It was determined that there was no harmonized approach in management of critical infrastructure in the East African region. It was further highlighted that there is a need to develop Regional harmonized guidelines on the management of Critical infrastructure.

To this end, EACO Working Group two (WG2) on_Infrastructure Development, Connectivity, Sharing and Digital Inclusion was assigned the task of developing guidelines on management of critical infrastructure within the East African region.

1.1 JUSTIFICATION

The need for these guidelines was driven by the existing risks and challenges affecting communications infrastructure in the region. These include;

i. Lack of planning and coordination that make it easy for destruction of Critical Infrastructure;

ii. Existence of human activities that cause destruction of critical communications infrastructure e.g. mining, construction, agriculture activities etc;

iii. Accidental or Technical failures that include infrastructure and hazardous material failures, power-grid failures, water-treatment facilities failures, water-mains ruptures, safety-systems failures and a host of other disasters of omission and/or commission;

iv. Cultural resistance and community hostilities leading to vandalism;

v. Lack of functional legal framework for protection of critical communication infrastructure as a critical resource;

vi. Political conflicts that lead to destruction of telecom infrastructure;

vii. Poverty where societies take infrastructure for scrap business;

viii. Limited awareness on the criticality of communication infrastructure;

ix. Terrorism related activities;

x. Natural disasters like flooding and earthquakes, tsunamis, land shifting, volcanic eruptions, extreme weather (hurricanes, floods, draught), fires; and

xi. Cyber-attacks that include the use of spam, phishing, and spyware/malware, on-demand industrial espionage.

2.0 Objectives

The main object of this assignment is to develop guidelines for managing critical communication infrastructure in the East African Community (EAC) region.
The specific objectives include:

i. To define the term critical infrastructure related to communication services for the EACO member states;
ii. To identify the most Critical Communications Infrastructure; and
iii. To develop guidelines for managing Critical Infrastructure.

3.0 Expected outcomes

The expected outcomes of this guiding document are:

i. Harmonized approach on protection of critical infrastructure in the East African Community (EAC) region;
ii. Service availability and good QoS;
iii. Protection of data;
iv. Mitigation of the vulnerability of critical communication infrastructure assets in EAC;
v. Establishment of a coordinated approach to the management of critical infrastructure in the event of natural disasters;
vi. Establishment of a coordinated approach in creating public awareness of the importance of critical infrastructure; and
vii. Identification and documentation of threats and hazards to the nation's critical infrastructure.

4.0 Critical Infrastructure

For purposes of this guideline, Critical Communications infrastructure shall mean an asset, facility, system or part thereof whether physical or virtual which is essential for the delivery of communication services in the EAC member countries, and whose disruption, degradation or destruction would have a significant impact on the security, governance, social and economic wellbeing of the society.

Based on the above definition, number of communications infrastructure have been identified as critical including but not limited to the following:

1. Intelligent Networks Systems e.g Revenue assurance;

2. CERTs;
3. Transmission network (microwave, Submarine cable, Fiber, satellite);
4. Data centers;
5. Mobile money Platforms;
6. Passive infrastructure;
7. Core network elements (HLRs, Gateway, Mobile Switch Center etc);
8. Radio Access Network;
9. IXPs; and
10. Broadcasting Networks.

To ensure accuracy and completeness, EACO members provided list of Critical communications infrastructure. Details of identified critical infrastructure provided by EACO members are contained in **Annex 1**.

5.0 CASE STUDIES IN THE MANAGEMENT OF CRITICAL COMMUNICATIONS INFRASTRUCTURE

Different jurisdictions have developed approaches in the management of critical communications infrastructure. Some of these include:

5.1 EUROPEAN UNION

The European Program for Critical Infrastructure Communication of 12th December 2006 set out an overall policy approach and framework for critical infrastructure protection (CIP) activities in the EU member states. 1 Body of European Regulators for Electronic Communications (BEREC) also recognized the rationale for the proposal to collect all critical infrastructure under one security framework.

5.2 KENYA

The Government of Kenya under Computer Misuse and Cybercrimes Act, 2018 designated infrastructure in the telecommunications sector as critical and identified categories of systems designated as critical infrastructure to include:

a) Voice/Data communication

-Mobile Communication Infrastructure/systems (Cellular base stations, communication links, cellular network components).

b) Internet Connectivity

-International Internet Gateways (Satellites, Cable Landing Sites/station).

-Broadband Networks (GCCN, NOFBI, ISPs Fiber Networks).

[1] https://ec.europa.eu/home-affairs/e-library/glossary/european-programme-critical_en

- Internet Exchange Points (IXP). Mobile Internet Networks (communication Network links and components)

c) Domain and IP Management

-Systems supporting DNS and IP functions and management of national, dot ke country code top level domain (.ke ccTLD) and dot ke (.ke) enterprise level domains.

d) Data and Information Management

-Data Centres/in-country cloud Infrastructure (GDCs, Africa Data centres, NRO1 data centre etc).

-Electronic Mail Systems and platforms centrally hosting and or processing emails as a service.

-Systems and platforms centrally hosting and/or processing data/information.

-Systems managing telecommunication Services quality assurance (QoS).

5.3 ITU

ITU's standardization sector contributes to the development of critical standards that enable the creation of more secure and robust ICT devices. ITU-T study group 17 has produced over 330 recommendations, many of which are related to cybersecurity. Topics on the cybersecurity standardization agenda have included: cybersecurity, cloud computing security, online analytics, internet-of-things security, smart-grid security, software-defined networking security, mobile security, intelligent transportation system security, anti-spam technical measures, identity management, public-key infrastructure, Privacy/personally identifiable information(PII), security architecture, information security management, telebiometrics, secure e-mail and application security.

6.0 GUIDING PRINCIPLES ON MANAGEMENT OF CRITICAL COMMUNICATION INFRASTRUCTURE IN EAST AFRICA

1. Put in place a National Communications Infrastructure database containing; list, location and ownership of critical infrastructure;
2. Develop back up and redundancy systems for all critical communication infrastructure;
3. Put in place remote monitoring and physical security controls;
4. Put in place disaster recovery plans including early warning systems;
5. Have Cyber security measures in place including CERTS among others;

6. Put in place alternative Power supply systems by using environmental friendly sources;
7. Decentralization of networks to improve resilience and minimize single points of failure;
8. Formulation of National legal and regulatory frameworks for Critical Infrastructure;
9. Establish Collaboration and partnerships between government and private sectors in joint effort to protect critical communication infrastructure;
10. Capacity building to obtain a skilled work force in management of critical communication infrastructure;
11. Put in place public awareness programs to protect critical communication infrastructure;
12. Member state to establish National and sectoral incident, crisis, and information sharing agreements policies.

7.0 Conclusion

EACO response to protection of critical communication infrastructure is set out as part of the objective of making member states more resilient to cyber-attacks, destruction and being well equipped in the management of critical communication infrastructure. Member states are therefore encouraged to adopt and implement these guidelines.