COMISSÃO DA CEDEAO
COMMUNIDADE DOS ESTADOS DA
AFRICA DO OESTE

ECOWAS COMMISSION
ECONOMIC COMMUNITY OF
WEST AFRICAN STATES

COMMISSION DE LA CEDEAO
COMMUNAUTÉ ECONOMIQUE
DES ETATS DE L'AFRIQUE DE
L'OUEST

ECOWAS Cybersecurity Agenda

"Enhancing Cybersecurity ECOWAS Region"

General Concept

1.1 Introduction

Today, Information and Communication Technologies (ICTs) have become an integral part of modern societies and are omnipresent, constantly transforming lifestyles. ICTs provide real time borderless communication and almost unlimited access to a range of services. Technical developments have improved daily life such as online banking, Mobile Data Services and Voice over Internet (VoIP) telephony, etc.

The availability of ICTs and network-based services offer a number of advantages for the society in general. ICT applications, such as e-Government, e-Commerce, e-Education, e-Health and e-Environment, are considered as enablers for socio-economic development, particularly due to their ability to deliver a wide range of basic services in remote and rural areas. In this regard, ICT applications can facilitate the achievement of Sustainable Development Goals (SDGs) in ECOWAS countries (Benin, Burkina Faso, Cabo Verde, Côte d'Ivoire, The Gambia, Ghana, Guinea, Guinea Bissau, Liberia, Mali, Niger, Nigeria, Senegal, Sierra Leone, and Togo).

The development of cheaper infrastructure technologies has enabled developing and Least Developed Countries to offer Internet services to more people. The popularity of the Internet and its services is growing fast: by the end of 2013 it is estimated that 39% of the world population (2.7 billion people) will be using the internet.

Today, we are more interconnected than ever before and overall reliance on the Internet continues to increase. Unfortunately, in this environment cyber-attacks occur rapidly and spread across the globe in minutes without regard to borders, geography, or national jurisdictions. Worldwide, every second, 18 adults become a victim of cybercrime, resulting in more than one-and-a-half million cybercrime victims each day. Cybercrime ranges from the stealing of private identity or child pornography distribution to the damaging and complete disruption of a country's Internet connectivity.

According to the 2015 report of the "Direction de l'Informatique et des Traces Technologiques" of Côte d'Ivoire, the overall financial damage of cybercrime is estimated to ***USD 6,636,530*** and the Nigeria Government reported a yearly loss of ***USD 399,560,000***

Consequently, it is crucial to prevent cyberspace from turning into a source of danger for users - state, business and citizen - and to build confidence and security ICTs' use: in other words to create a safe cyber environment - to ensure cybersecurity.

1.2 Problem statement

ICTs provide unprecedented opportunities to accelerate social and economic development, while at the same time, the misuse of ICTs and their vulnerabilities create new and serious threats having the potential to harm the society.

This major threat to all the developed as well as the developing countries such as ECOWAS Member States presents a growing need to be able to communicate, coordinate, analyze, and respond to cyber-attacks across different business sectors at national, regional and global levels.

To answer the challenges imposed by the borderless nature of cybercrime and to achieve cybersecurity worldwide, establishment of national cybersecurity strategies including mechanism to identify, manage and respond to cyberthreats as well as cooperation between countries at regional and international levels is crucial.

This is particularly challenging for ECOWAS countries lacking of adequate implementation of the adopted legal and regulatory framework, limited human capacity/expertise and financial resources.

1.3 Justification

In a context of ever increasing growth of malicious cyberactivities, the cybersecurity Project aims for assistance to the ECOWAS region and its Member States to protect their cyberspace and critical information infrastructure as well as at building confidence and security in ICTs' use. It also aims at providing the Member States with the capacity of participating effectively in the global effort to fight cybercrime including cyberterrorism.

The project will be implemented in the framework of the ECOWAS mandate to implement Supplementary Acts on Electronic Transactions, Personal Data Protection and Directive on fighting Cybercrime, as well as the action line C5 of the Plan of Action of the World Summit on the Information Society (WSIS) and and International instruments such as the Budapest Convention.

2. Description

2.1. Objectives

The ECOWAS Cybersecurity Agenda "Enhancing Cybersecurity in ECOWAS region" aims at supporting the Member States in strengthening their cybersecurity capabilities to better respond to cyberthreats to ensure enhanced protection of their national infrastructure, including the critical information infrastructure, thereby making the Internet safer and protecting Internet users, to serve national priorities and maximize socio-economic benefits in line with the objectives of the World Summit on the Information Society (WSIS) and for Sustainable Development Goals (SDGs).

The Project will contribute to harmonization, consolidation and support the regional cybersecurity and the specific objectives are:

1. Enacting and implementation of Cyber legislations in the Member States
2. Assessment of cybersecurity current status in Member States;
3. Audit of the existing Computer Emergency Response Teams (CERTs) in the Member States and upgrade them if necessary
4. Establish CERT in the Member States where it does not exist
5. Fight against cybercrime
6. Training of the policy makers, regulators, judges, prosecutors, police, investigators and security officers;
7. Raise awareness of all stakeholders involved in cybersecurity issues including users
8. Explore the possibility of establishment and operation of the Regional Cybersecurity Centre
9. Deploy PKI facilities and adopt PKI regulations;

2.2. Expected results:

The expected results of the Project include:

- Implementation of the adopted Cyber legislations in the 15 Member States
- Adoption complementary legislation when needed
- CERT upgrade or established in the Member States
- Enhanced national expertise on cybersecurity including, among others, technical, legal and regulatory, institutional and organizational aspects;

- Training activities on cybersecurity and cybercrime aspects;
- Improved national preparedness in identification, prevention, response, and resolution of cybersecurity threats/incidents including cyberterrorism;
- Customized Community Texts on national cybersecurity legislation, regulation and technical aspects;
- Cybersecurity strategy adopted including child online protection
- Training curricula developed on cybersecurity national, regional and international legislation, regulation and technical aspects
- More security in the ECOWAS region including in the cyber space

2.3. Implementation strategy/methodology

Cybersecurity is a surging concern for everyone; Governments, Civil Societies and the Private sector as well as larger International Community. Therefore, there is a need to have a shared responsibility to combat cybercrime

In order to assist ECOWAS Member States to fast track the implementation of their cybersecurity programme, including among others, establishment of CIRT/CERT, awareness and capacity building of the stakeholders (Technical Experts, Judiciary, Parliamentarians, Police/Law Enforcement, etc.), the ECOWAS Commission is partnering for financial support to implement its Cybersecurity Agenda to contribute in building trust and security in the digital world and fighting against cybercrime.

2.4 Sustainability

As the ECOWAS Cybersecurity Agenda will be implemented on inclusive basis, adoption of regional and national cybersecurity strategy and adequate training conducted for all stakeholders involving in the cybersecurity and cybercrime issues, ECOWAS Member States will be able to not only sustain their national strategy after the assistance period but also develop enough skill to fight against all type of cyber threats.

3. Estimated cost

Cybersecurity and cybercrime issues are continued process as networks are growing fast and cyber threats are also getting more technically sophisticated and the tools are readily available. Therefore, no estimated cost is provided in this document.

ECOWAS is in the process of mobilizing fund for the implementation of its Cybersecurity Agenda. In addition to internal funds, ECOWAS will define the contribution of the Partners based on the selected activities they intend to support as part of the ECOWAS Cybersecurity Agenda.

- **Location:** ECOWAS 15 Member States
- **Total estimated budget for the activities below is estimated to:** XXX

Below are some identified projects/activities associated with the ECOWAS Cybersecurity Agenda

Projects/Activities	Cost
Cybersecurity assessment in the 15 Member States including CERT assessment	
Establishment and operation of a Regional Cybersecurity Centre	
CERT implementation or upgrade/enhancement of existing CERT	
Capacity building/Trainings of key stakeholders	
Capacity building for Experts from Member States on Cyberdrill	
Cybersecurity strategy including Child online Strategy and Projects	
Develop necessary cyber legislation	
Assistance in implementation of adopted Cyber legislation in Member States	
Development of regional and national Cybersecurity Strategy	
Collaboration globally to fight against cybercrime	
Deployment of PKI and development of PKI regulation	
Regional Report for ECOWAS Region	
Total cost	