ECOWAS Regional Cybersecurity and Cybercrime Strategy

SECTION I. INTRODUCTION

The rapid digital transformation underway in West Africa is of great importance to improve the functioning and efficiency of administrations, public policies and economies, as well as the well-being of populations. However, the growing threats and risks facing global cyberspace and digital networks, information systems and data can significantly reduce the expected benefits of these digital policies, and seriously harm the interests of Nations, their economies, institutions and people.

Faced with these threats and risks, robust national cybersecurity and anti-cybercrime organisations should be put in place, with good coordination between the departments concerned, effective response mechanisms to cyberattacks, experts and users of digital services sensitized and trained in good practices, active private sector participation, enhanced protection of the most essential or critical digital services and infrastructure, as well as regional mutual assistance and international cooperation.

Clearly, these requirements are still far from being met within the region. Some countries have already set up the necessary institutions and reached a certain degree of preparation, most of the others are still at an insufficient level, constituting a weakness endangering their Nation as much as the rest of the region. In addition, all countries face a shortage of expertise in these areas. All countries are therefore encouraged to develop cybersecurity curricula and to reach a minimum level in cybersecurity and the fight against cybercrime.

Furthermore, the heterogeneity of the systems in place in the different countries considerably limits any attempt at regional cooperation. Their harmonization must therefore be sought: links and exchanges would be easier and more effective between institutions with perimeters of comparable responsibilities and operating modes; identical requirements and procedures would also ensure the protection of transnational infrastructures in the same way across the region; finally, harmonized penal and criminal procedure provisions would enable an efficient mutual assistance in criminal matters.

In this area, ECOWAS has implemented harmonization provisions since 2010: in particular, Supplementary Act A/SA.1/01/10 on personal data protection within ECOWAS sets out the security obligations incumbent on those responsible for processing such data to ensure confidentiality; Supplementary Act A/SA.2/01/10 on electronic transactions within ECOWAS sets the conditions for acceptance of electronic signature; Lastly, Directive C/DIR 1/08/11 on fighting cybercrime within ECOWAS adapts the substantive criminal law and the criminal procedure of Member States to address the cybercrime phenomenon.

At the continental level, the 2014 African Union Convention on cybersecurity and personal data protection, known as the Malabo Convention, sets out the cybersecurity and cybercrime measures to be taken at national level. At the global level, the 2001 Convention on Cybercrime, known as the Budapest Convention, open for signature by all countries, aims to pursue a common criminal policy by adopting suitable legislation, intensify cooperation between Member States in criminal matters and adopt powers sufficient for effectively fighting cybercrime.

The objective of this Regional Strategy is to make the most of these advances, to improve the level of national cybersecurity and cybercrime mechanisms, and to develop cooperation and mutual assistance between the countries of the region. It draws on internationally recognized best practices in these areas.

These objectives must be achieved without prejudice to the fundamental freedoms and human and peoples' rights contained in the declarations, conventions and other instruments adopted at regional, continental and international level.

SECTION II. GENERAL CONSIDERATIONS

A. Overall objective

The overall objective of this Strategy is to establish a community strategic framework to be considered by Member States in their national strategies and implemented in their action plans on cybersecurity and the fight against cybercrime before the end of 2022, with the full participation of the ECOWAS Commission for the benefit of this Community Member States.

B. Definitions

For the purposes of this Regional Strategy, the following definitions shall apply:

Critical Infrastructure: a public or private infrastructure or process whose destruction, standstill, illegitimate exploitation or disruption for a defined period of time will cause either loss of lives or significant loss to the economy or damage significantly the reputation of the Member State or its symbols of governance. In this definition, infrastructure includes the networks, systems and the physical or digital data essential for providing this service. This term may refer to a certain system or process whose functioning is critical within the organization;

Critical infrastructure operator: public or private operator that operates a critical infrastructure;

Critical infrastructure protection (CIP): set of safeguards and actions to protect critical infrastructures from any risks and threats that could cause the total or partial interruption of the essential services they provide;

CSIRT (Computer Security Incident Response Team): team responsible for alerting about threats, preventing risks and threats to information systems, reacting to security incidents and aiding in mitigation;

Cyber hygiene: all the good practices that each digital player should respect in order to preserve the security of the information system that he uses or for which he acts as an administrator;

Cybercrime: criminal activities where computers and information systems are involved either as a primary tool or as a primary target. Cybercrime comprises traditional offences (e.g. fraud, forgery, and identity theft), content-related offences (e.g. on-line distribution of child pornography or incitement to racial hatred) and offences unique to computers and information systems (e.g. attacks against information systems, denial of service and malware);

Cybersecurity: set of safeguards and actions to protect the cyberspace and cyber assets from those threats that are associated with or that may harm its networks and information infrastructure. Cybersecurity strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein;

Cyberspace: the interdependent network of information systems infrastructures including the Internet, telecommunications networks, information systems and Internet of things;

Digital data: any representation of facts, information or concepts in a form suitable for processing in a computer system;

Essential service: a service where total or partial interruption of which could have a serious impact on the functioning of the Member State, the economy of the country or on the health, safety, security and well-being of citizens, or any combination of these issues that does not rise to the criteria of critical Infrastructures;

Essential service operator: public or private operator that provides an essential service;

Essential services protection: set of safeguards and actions to protect essential services from any risks and threats that could cause their total or partial interruption;

Information and communications technologies (ICT): technologies used to gather, store, use and send information, including technologies that involve the use of computers and any communication system, including any telecommunication system;

Information system: any isolated or not isolated device or group of interconnected devices that all or in part carries out automatic processing of data pursuant to a program;

Networks: set of means ensuring the supply of an infrastructure with products or services necessary for its operation (communications, energy, logistics, etc.).

SECTION III. STRATEGIC OBJECTIVE 1: FORMULATE NATIONAL CYBERSECURITY AND CYBERCRIME POLICY AND STRATEGY

Each Member State should adopt and update at least every five years national cybersecurity and cybercrime policy and strategy[1], considering this Regional Strategy, which sets for each of these two domains:

- The situation of the country and the challenges it faces;
- The political vision of the country;
- The strategic objectives to be achieved, deadlines and priorities;
- The national governance, roles and assignment of responsibilities;
- The objectives in terms of:
    - strengthening of legislative and regulatory provisions;
    - standards and requirement rules;
    - security for critical infrastructure and essential services;
    - strengthening the institutional framework;
    - technical capacities and skilled human resources to be acquired;
    - awareness, communication, education and training;
    - threat prevention and risk management;
    - security incidents report;
    - detection and attribution of attacks;
    - response in case of an attack;
    - development of a cybersecurity and cybercrime ecosystem;
    - synergy in actions at the national level (national dialogue and coordination);
    - regional and international cooperation;
- Actions to be taken to achieve these objectives, the stakeholders to be involved, the deadlines to be met and estimated budgets;
- Means to strengthen institutions and capacities and to ensure their sustainability.

Each Member State should define a monitoring and evaluation mechanism for the actions planed by its national cybersecurity and cybercrime strategy and implement it at least annually.

SECTION IV. STRATEGIC OBJECTIVE 2: STRENGTHEN CYBERSECURITY FOR A SAFE AND SECURE CYBERSPACE

Sub-objective 2.1. Establish a national cybersecurity Authority

Each Member State should establish and designate a national cybersecurity authority with the necessary powers and means to perform the following functions, either directly or by delegation of a governmental (and if possible inter-ministerial[2]) authority:

[1] National policy and national strategy can be two separate documents, or a single document of national strategy which describes the country's political vision and objectives.

[2] However, it is recommended that smaller to medium Member States establish a central authority, that will work with all the other Ministries because of the lack of resources, and due to the quick changes and need to be up to speed, as sometimes creating big inter-ministerial committees may hamper progress.

- Global governance of the national cybersecurity (definition of national and sectoral cybersecurity policies, elaboration of the national and sectoral strategies, follow-up of the action plans, elaboration of legislative and regulatory texts, coordination of tasks related to cybersecurity, management of prevention and response mechanisms, facilitation of the interactions with public and private stakeholders, etc.);
- Facilitation of the national cybersecurity framework, notably through the national CSIRT;
- Coordination with the authorities responsible for fighting cybercrime;
- Transposition of the ECOWAS acts on cybersecurity into national texts;
- Monitoring of the proper implementation of international Conventions, ECOWAS acts, the Regional Strategy and the national laws and regulations on cybersecurity;
- Serve as the main point of contact for regional and international cooperation.

The national cybersecurity authority must be able to exercise its mission over all sectors (Member State services, telecommunications, energy, health, transport, banks, etc.), in liaison with the relevant sectoral authorities and without prejudice to the powers devolved to these authorities.

Sub-objective 2.2. Establish alert and incident response capabilities (CSIRTs)

Each Member State should have a national CSIRT:

- Primarily covering Member State services, critical infrastructures and essential services (the "priority beneficiaries");
- In charge of facilitating and coordinating the sectoral CSIRTs network, seeking all possible synergies and subsidiarity;
- Able to perform at least the following functions:
  - Search and disseminate alerts and warning (vulnerabilities, risk, incidents), threat circumvention measures, guides and best practices;
  - Track national incidents;
  - Handle incidents affecting priority beneficiaries;
  - Participate in the regional and global CSIRT networks;
  - Coordinate reactions and crisis management in liaison with authorities in case of major incident;
  - Acquire services of relevant intelligence feeds;
  - Incorporate relevant systems and technologies to quickly collect and analyse relevant data;
  - Establish a call centre for reporting cyber-attacks;
- Equipped with the necessary resources (financial, security of premises and IT systems, sufficient staff to ensure permanent availability, competent staff, forensic capacities, procedures, website ...).

Each Member State should encourage the establishment of sectoral CSIRTs, in particular to ensure, in a shared manner for the benefit of operators in certain sectors of activity, the research and dissemination of alerts on the digital systems and applications specific to these sectors of activity, and the incident handling. It is recommended that CSIRTs are located in the same location to ensure open dialogue and inter sectoral enrichment.

Sub-objective 2.3. Establish a risk management approach

Each Member State should adopt and have each operator concerned adopt a risk management approach, both at the strategic level and within public and private bodies, to ensure the security of networks, information systems and digital data at the appropriate level.

Each Member State should ensure that those in charge of cybersecurity, at all levels, receive the necessary hierarchical support so that their assessments and recommendations will be considered by the decision-makers.

Sub-objective 2.4. Strengthen cybersecurity for critical infrastructure and essential services

Each Member State should prioritize its cybersecurity efforts on its critical infrastructure and essential services.

Each Member State should have a procedure for identifying networks, information systems and digital data essential for the operation of critical infrastructure and the provision of essential services.

Each Member State should impose on public and private operators who are responsible for critical infrastructures and essential services concrete measures to ensure the security of these networks, information systems and digital data, including the following minimum measures:

- compliance with internationally recognized cyber hygiene measures;
- a security audit of information systems by a qualified body, at a frequency not exceeding two years;
- notification of security incidents to the national cybersecurity authority or to the national CSIRT (via its possible sectoral CSIRT).

Sub-objective 2.5. Adopt information security policies

Each Member State should require public authorities and critical infrastructure and essential services operators, as well as recommend to other operators to develop and apply security policies describing the measures they lay down for ensuring security of their information systems (responsibilities, organisation, dedicated human resources, cybersecurity equipment, protection procedures, detection and response to attacks, etc.).

Sub-objective 2.6. Develop a general security baseline

Each Member State should develop a General Security Baseline setting the minimum information security requirements (governance, organization, information security policy, system mapping, technical requirements, etc.) and designate in a document with legal force to the bodies which are subject to it.

Sub-objective 2.7. Enhance cybersecurity skills development

Each Member State should develop a qualified human workforce trained in different aspects of cybersecurity, this may be done by:

- introducing training courses in the various areas relating to cybersecurity (technical, legal, etc.) in its teaching programs, in particular university and professional;
- promoting the enhancement of cybersecurity skills among all information and communication technology professionals;
- promoting research and innovation in the field of cybersecurity;
- embedding cyber security proven knowledge requirements in government tenders for services.

Sub-objective 2.8. Ensure development of the cybersecurity offer

Each Member State should ensure the creation of public and private bodies capable of providing assistance to operators in the field of cybersecurity (providing secure solutions, securing information systems, consulting, auditing, incident handling, etc.).

SECTION V. STRATEGIC OBJECTIVE 3: REDUCE CYBERCRIME INCIDENTS WITH AN ENABLED ENVIRONMENT AND CAPABILITY TO BRING PERPETRATORS TO JUSTICE

Sub-objective 3.1. Adopt penal and procedural provisions

Each Member State should adopt the penal and procedural provisions prescribed or recommended at regional, continental and global level.

Each Member State should adopt proportional sanctions for criminal offenses which have affected or attempted to affect the information and data systems necessary for the proper functioning of critical infrastructure and essential services.

Sub-objective 3.2. Build capacities against cybercrime

Each Member State should equip itself with the following minimum capacities to fight against cybercrime:

- At least one operational cybercrime unit;
- A coordination authority if there are two or more operational cybercrime units;
- At least one investigative laboratory;
- Digital evidence collection capabilities;
- Procedures for digital investigation and collection and handling of digital evidence;
- Member State investigators (judicial police officers and agents, judicial experts, etc.) trained in digital investigations and digital evidence collection and handling;
- Magistrates trained in the investigation and adjudication of cybercrime cases.

SECTION VI. STRATEGIC OBJECTIVE 4: PROMOTE COORDINATION AND COOPERATION IN ENHANCING CYBERSECURITY AND FIGHTING CYBERCRIME

Sub-objective 4.1. Promote ratification of conventions

Each Member State should ratify the necessary regional, continental and international conventions on cybersecurity and cybercrime.

Sub-objective 4.2. Ensure promotion of the cybersecurity culture

Each Member State should develop a cybersecurity culture, using all possible means (government communication, seminars, media, school, university and continuing education, etc.) to achieve the following objectives:

- Everyone's awareness of cyber threats;
- Promotion of digital hygiene and other good IT practices among the general public;
- Awareness among public and private decision-makers of their roles and responsibilities;
- Warning citizens about the penalties for the commit of cybercrime.

Sub-objective 4.3. Ensure national coordination

Each Member State should mobilize all public and private actors to promote and develop dialogue, coordination and synergies among all stakeholders, including:

- authorities and institutions responsible for cybersecurity or the fight against cybercrime;
- critical infrastructure operators;
- suppliers of cybersecurity or secure products;
- cybersecurity service providers;
- training and research institutions;

- civil society organisations;
- media.

Sub-objective 4.4. Promote regional and international cooperation

Member States and the ECOWAS Commission should promote and develop regional and international cooperation among cybersecurity and cybercrime authorities and institutions:

- In the field of capacity building: share good practices and develop intraregional synergies and mutualisation, especially in the area of training;
- In the institutional field: harmonize the strategies, organisations and procedures of the countries of the region, particularly with regard to security of transnational critical infrastructures and the fight against cybercrime;
- In the operational area: share alerts and cybersecurity information especially between national CSIRTs, organize joint responses, pool intervention resources in order to fight potential or proven cyber threats and cybercrime as effectively as possible;
- In the judicial field: ensure international judicial cooperation in cybercrime and transnational access to digital evidence;
- Establish a regional cyber security simulation and training centre to cut costs and promote interoperability;
- Joint information sharing organisations should be encouraged in the critical and essential services (energy, finance, health, etc.);
- Create mechanisms and joint MOUs with other information sharing organizations.

SECTION VII. STRATEGIC OBJECTIVE 5: ESTABLISH REGIONAL MECHANISMS

Sub-objective 5.1. Establish a regional assistance plan for the implementation of the Regional Strategy

In order to help the Member States to implement this Regional Strategy, the Commission will implement, with the means at its disposal, the regional action plan set out in the annex.

Sub-objective 5.2. Establish a regional Strategy monitoring system

ECOWAS Commission will explore with Member States the possibility of setting up a sustainable Regional Technical Committee (RTC), composed of a high-level representative provided by each Member State, placed under the coordination of the ECOWAS Commission and meeting at least once a year, to ensure over time the monitoring of the provisions of this Strategy and to propose the necessary new actions.

Sub-objective 5.3. Establish a cybersecurity Coordination Centre

The ECOWAS Commission will explore with Member States the desirability of creating, in the short or medium term, an ECOWAS Cybersecurity Coordination Centre, responsible in particular for coordinating the various capacity-building initiatives carried out in the countries in the area of cybersecurity and cybercrime, and for organizing, where possible, pooling and sharing of results between countries.

In the longer term, it may consider setting up a regional agency to promote and facilitate regional cooperation in the area of cybersecurity and the fight against cybercrime.

Sub-objective 5.4. Identify and pursue funding for national cybersecurity and cybercrime arrangements

The ECOWAS Commission, in liaison with the Member States, will explore the possibilities of harmonizing, within ECOWAS, mechanisms for funding national cybersecurity and cybercrime arrangements, especially with regard to public-private partnerships.

The ECOWAS Commission, in liaison with Member States, will seek funding from donors to address the unmet priority needs of these Member States.