ECOWAS COMMISSION
COMMISSION DE LA CEDEAO
COMISSÃO DA CEDEAO

NINETY-THIRD ORDINARY SESSION OF THE COUNCIL OF MINISTERS

Abuja, 13 December 2024

DIRECTIVE C/DIR.2/12/24 ON CYBER/ICT CONFIDENCE BUILDING MEASURES (CBMs)

THE COUNCIL OF MINISTERS,

MINDFUL of Articles 10, 11 and 12 of the ECOWAS Revised Treaty as amended establishing the Council of Ministers and defining its composition and functions;

MINDFUL of Articles 27, 32 and 33 of the ECOWAS Revised Treaty, on science and technology, and communication and telecommunications;

MINDFUL of Supplementary Act A/SA.1/01/07 on the harmonization of policies and regulatory framework of the Information and Communication Technology (ICT) Sector;

MINDFUL of Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS;

MINDFUL of Supplementary Act A/SA.2/01/10 on Electronic Transactions within ECOWAS;

MINDFUL of Directive C/DIR.1 /08/11 on Fighting Cybercrime within ECOWAS;

MINDFUL of the Directive C/DIR.1/01/21 Relating to the adoption of the Regional Cybersecurity and Cybercrime Strategy;

MINDFUL of the Directive C/DIR.2/01/21 adopting the Regional Policy for Critical Infrastructure Protection in ECOWAS;

CONSIDERING the rapid advancement of Information and Communication Technologies (ICTs) that has transformed cyberspace into a complex environment and exposed nations to significant cyber threats from both state and nonstate actors;

CONSIDERING ALSO that these threats are increasingly frequent and have transnational impacts, including the potential to disrupt critical infrastructure and spread disinformation;

AWARE that Confidence Building Measures (CBMs) serve as essential tools for fostering international cyber stability by enhancing cyber resilience through international cooperation and inter-agency coordination;

RECOGNIZING the necessity for transparency, co-operation, confidence and capacity building between ECOWAS Member States in cyberspace to ensure stability and growth in the region;

BEARING IN MIND the reports of the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security; the Open-ended working group on developments in the field of information and telecommunications in the context of international security; and the Open-ended Working Group on security of and in the use of Information and Communications technologies;

NOTING that the effective operationalization and reinforcement of CBMs are vital and key to an open, secure, stable, and peaceful ICT environment;

CONSIDERING the need to enhance Member State's transparency and co-operation in the use of Information and Communications Technologies (ICTs) to reduce its malicious use;

DESIROUS of adopting confidence-building measures (CBMs) to guide Member State's behaviour and promote stability in the global cyber landscape;

ON THE RECOMMENDATION of the 19th Meeting of Ministers in charge of Telecommunications, ICT and Digitalisation of ECOWAS Member States held in Cotonou, from 2-4 October 2024;

UPON the opinion of the Parliament, through its Bureau, meeting in emergency session in Abuja from December 6 to 14, 2024, pursuant to Article 25 (B) (3) (vii) of the Supplementary Act A/SA.1/12/16 on the Enhancement of the Powers of the ECOWAS Parliament.

PRESCRIBES:

ARTICLE 1: CONFIDENCE BUILDING MEASURES (CBMs)

This **DIRECTIVE C/DIR.2/12/24** hereby prescribes the first set of Confidence-Building Measures (CBMs) as follows:

1. **CBM No. 1. Share information on Cybersecurity related documentation**
    a. Member States shall be encouraged to share information with other Member States on their national cyber security policies, strategies, regulations, best practices, threat perceptions and programmes in their chosen format and fora, as appropriate.
    b. Where possible and applicable, the providing Member state may declare or highlight possible alignment of the shared documentation, information, or best practice applied across the ECOWAS region.
2. **CBM No. 2. Designate National points of contact**
    a. Each Member State shall:

i. designate diplomatic and technical points of contact to support the coordination of communication and discussions about cybersecurity at the national, regional and international levels.

ii. be encouraged to ensure coordination at national level between the points of contact;

iii. be encouraged to provide and regularly update the contact details of their designated points of contact;

iv. be encouraged to establish measures to ensure timely and rapid exchanges in the event of national or international cyber security incidents;

v. be encouraged, where possible, to nominate the same Points of Contact as those in the UN global directory to facilitate national coordination.

b. These points of contact shall coordinate responses, whether diplomatic or technical in nature, and facilitate interactions between their respective national bodies;

c. The ECOWAS Commission shall serve as a facilitator of the points of contact network.

3. CBM No. 3. Raising awareness on cyber threats and remediation measures

a. Each Member State shall be encouraged to facilitate or participate in collaborative activities to raise awareness and enhance readiness against cyber security threats within their respective countries and the region.

b. The activities referred in paragraph a. above, can be directed towards national cyber security entities, experts or the public. These collaborative activities may include, but are not limited to:
   i. Social media campaigns with written and audio-visual components;
   ii. Radio, television or online interviews and notifications;
   iii. Round tables with experts aimed at target audiences;
   iv. Conducting printed awareness raising campaigns;
   v. Commissioning and distributing materials aimed at countering specific threats stemming from cyberspace.

c. Member States shall enhance cyber capacities, inter alia, through meetings, conferences, workshops and knowledge sharing.

d. Member States shall continue exchanging views within expert groups on the development and implementation of CBMs, including the potential development of additional CBMs.

ARTICLE 2: ESTABLISHMENT OF THE ECOWAS CYBER SECURITY WORKING GROUP

1. Member States shall be encouraged to establish an informal, Open-ended Working Group, composed of National cyber-security experts from all ECOWAS Member States within three (3) months from the date of entry into force of this Directive. The working Group shall be chaired by the expert from the Member State serving as Chair of the Authority.
2. The working group shall be encouraged to meet at least once a year to discuss progress, share insights and plan future initiatives.
3. The ECOWAS Commission shall serve as a secretariat and support the Chair to perform the following tasks:
    a. elaborate individual confidence-building measures aimed at enhancing transparency, co-operation, predictability and capacities necessary to reduce risks of escalation, misunderstanding and conflict stemming from the use of cyber/ICTs;
    b. approve elaborated CBMs by consensus and when appropriate, submit them for adoption;
    c. adopt Confidence-building measures with indicators and measurements of success;
    d. discuss the implementation and operationalization modalities of adopted confidence-building measures by ECOWAS Member States;
    e. provide annual reports to the Council of Ministers detailing progress on the adoption and implementation of confidence-building measures, in line with indicators of success;
    f. conduct discussions guided by the following principles:
        i. all confidence-building measures shall be applicable equally to all Member States, without discrimination based on cyber security capacity, geography, nationality or language;
        ii. while voluntary, all adopted confidence-building measures shall be understood and accepted on the level of individual Member States; and
        iii. confidence-building measures need to be synchronous with regional and national initiatives aimed at building cyber resilience, capacities and security in the ECOWAS region.
4. The Member States shall recognize that confidence-building measures are adopted and shall operate in a multistakeholder environment with governmental, non-governmental, private sector and other actors active in cyber security in the ECOWAS region.

ARTICLE 3: REVISION

1. This Directive shall be reviewed and amended as necessary to mitigate identified risks or to include additional identified CBMs.

2. The Directive may also be reviewed upon recommendation of any Heads of the Community Institutions.

ARTICLE 4: PUBLICATION

1. This **DIRECTIVE C/DIR.2/12/24** shall be published in the Official Journal of the Community by the Commission within thirty (30) days of its signature by the Chairperson of the Council of Ministers.

2. It shall also be published by each Member State in its National Gazette within same time frame.

ARTICLE 5: ENTRY INTO FORCE

This **DIRECTIVE C/DIR.2/12/24** shall enter into force upon its Publication.

DONE IN ABUJA, THIS 13TH OF DECEMBER 2024

.....

H. E. YUSUF MAITAMA TUGGAR (OON)

CHAIRMAN

FOR THE COUNCIL