



ECOWAS COMMISSION
COMMISSION DE LA CEDEAO
COMISSÃO DA CEDEAO

Cybersecurity and Cybercrime: A regional perspective



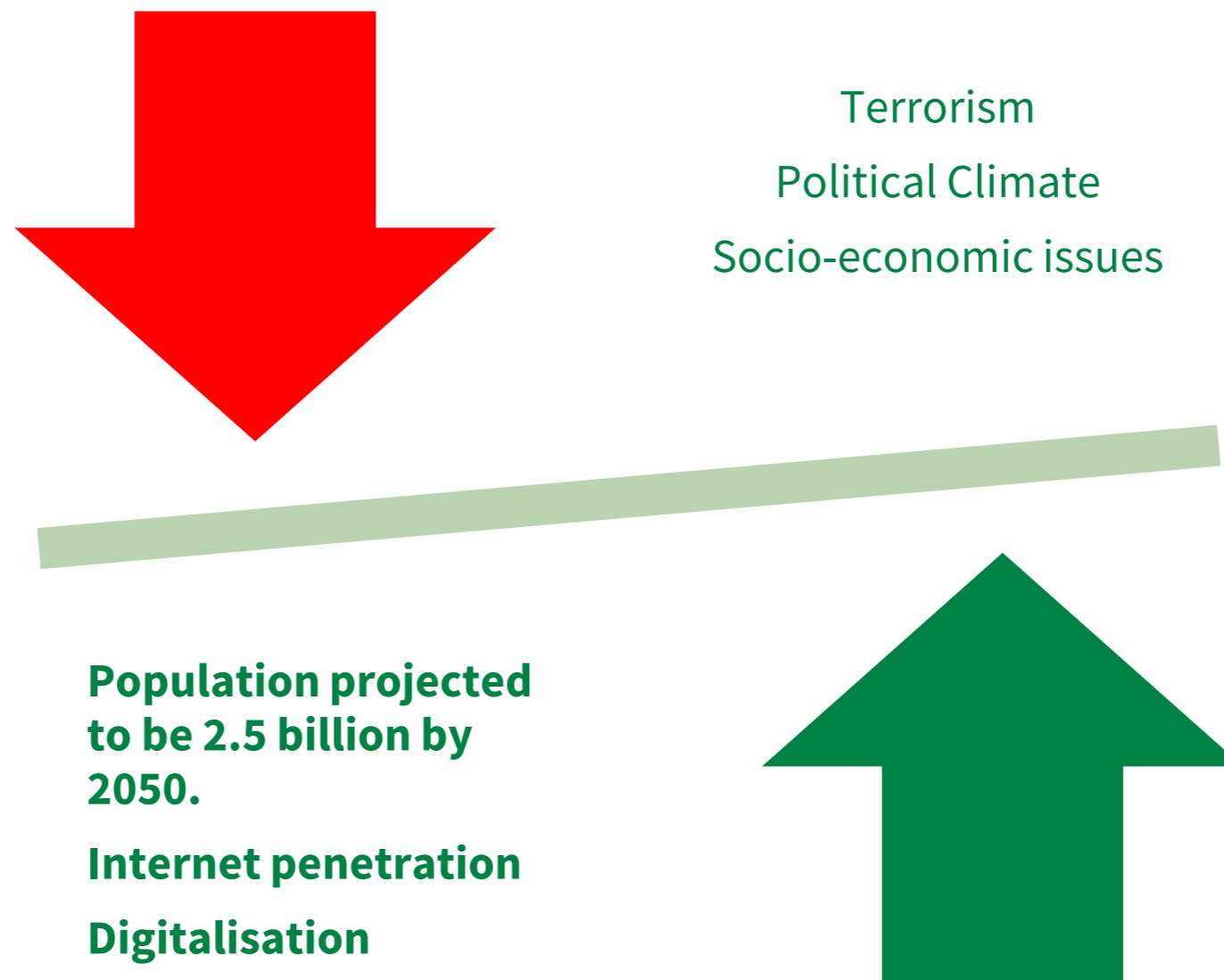
ECOWAS COMMISSION
COMMISSION DE LA CEDEAO
COMISSÃO DA CEDEAO

Outline

- A. Concerns
- B. ECOWAS Cybersecurity Agenda
- C. Current Situation
- D. Regional Instruments
- E. Way Forward



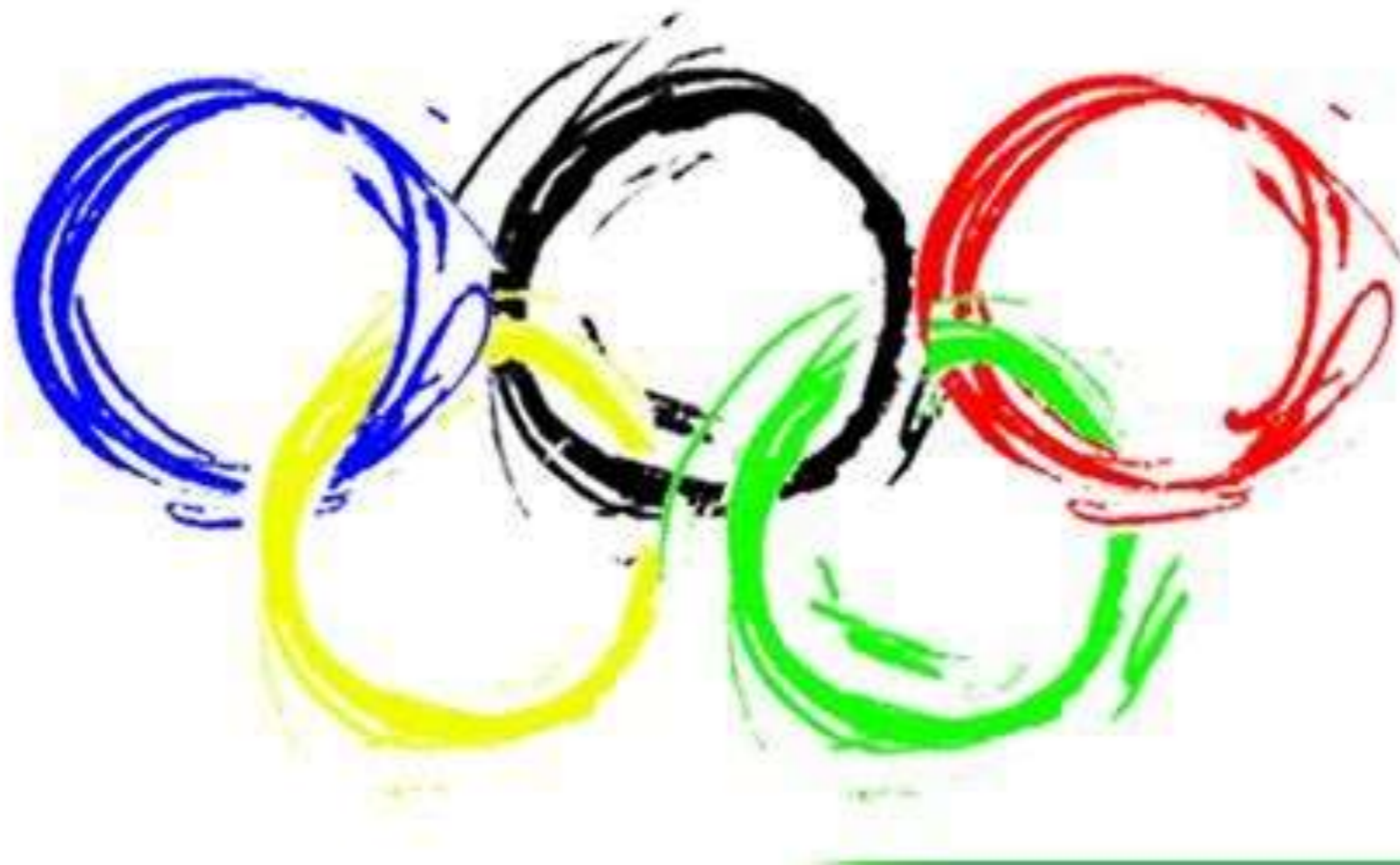
Snapshot





ECOWAS COMMISSION
COMMISSION DE LA CEDEAO
COMISSÃO DA CEDEAO

All





ECOWAS COMMISSION
COMMISSION DE LA CEDEAO
COMISSÃO DA CEDEAO

Cat and Mouse



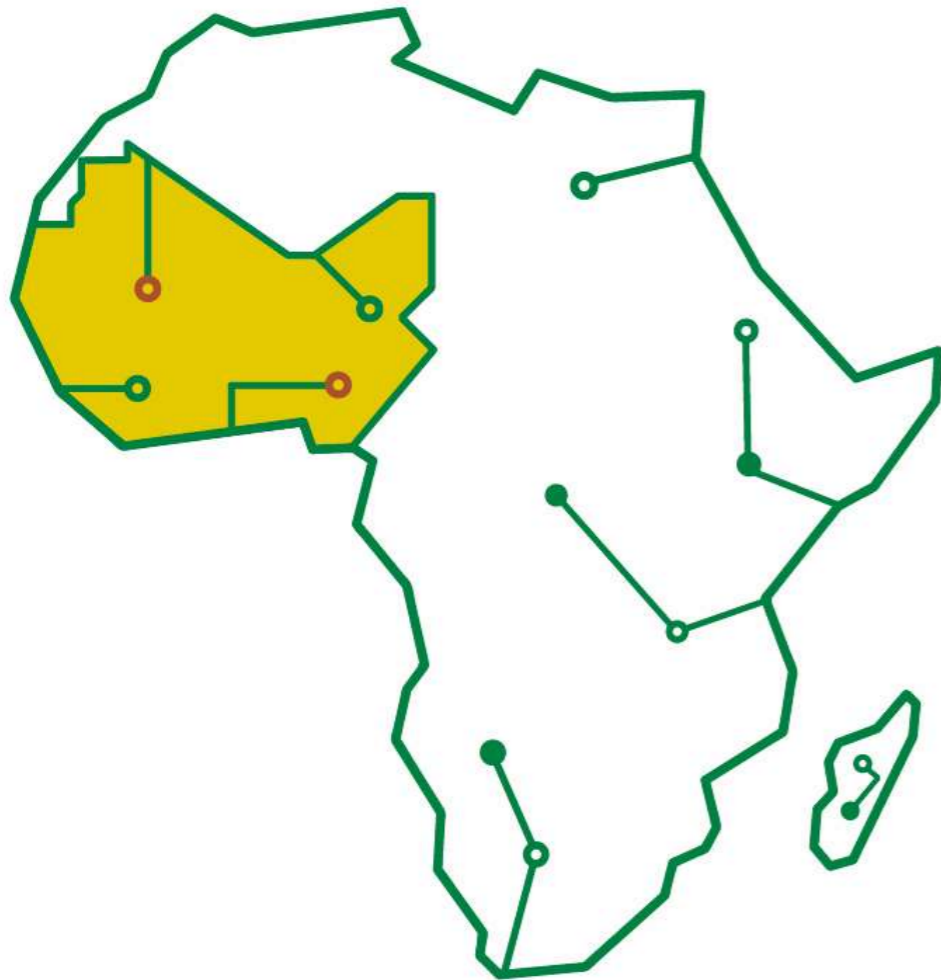


Are we being Vigilant?

ⓘ Start presenting to display the poll results on this slide.



Perhaps?



- 29 out of 54 (legislation)
- 52% of companies believed **unprepared** to handle a large-scale cyber-attack.
- **> 90%** of businesses (no necessary cybersecurity protocols.)
- losing \$4 billion annually to cybercrime

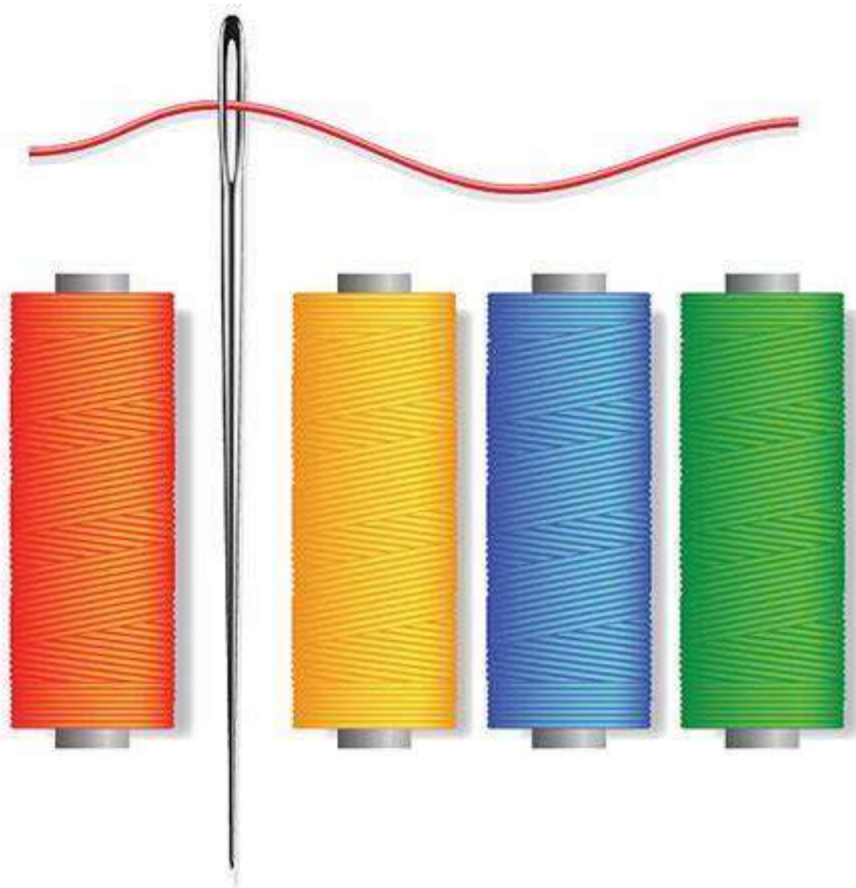


Prominent threats

- 1. Online scams**
- 2. Digital extortion**
- 3. Business Email Compromise (BEC)**
- 4. Ransomware**
- 5. Botnets**



Common Thread?



1. Angola
2. Benin
3. Botswana
4. Burkina Faso
5. The Gambia
6. Ghana
7. Kenya
8. Nigeria
9. Senegal
10. South Africa
11. Tanzania



BEC actors - Top 3 countries

① Start presenting to display the poll results on this slide.



ECOWAS COMMISSION
COMMISSION DE LA CEDEAO
COMISSÃO DA CEDEAO

A. Concerns/Challenges



ECOWAS COMMISSION
COMMISSION DE LA CEDEAO
COMISSÃO DA CEDEAO

Concerns/Challenges

- Awareness
- Rankings
- Resources
- Cooperation
- Priority
- Physical Security



ECOWAS COMMISSION
COMMISSION DE LA CEDEAO
COMISSÃO DA CEDEAO

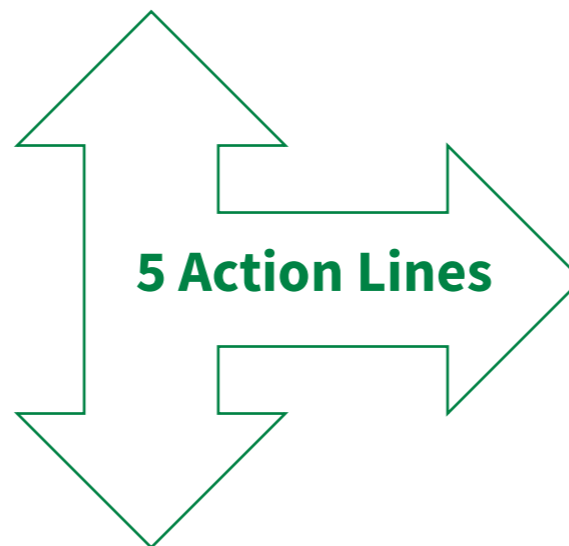
B. ECOWAS Cybersecurity Agenda



ECOWAS Cybersecurity Agenda

Pillar 1
Fight Cybercrime

Pillar 2
Improve
Cybersecurity
Environment



**Legislation/
Policy
Framework**

**Handle
Cybercrime**

Resilience

Capacity Building

**International
Cooperation**



Action Lines

Handle Cybercrime

- **Establish digital forensic laboratories**
- Develop Child Online Protection (COP) Strategy
- **Enhance the capabilities of operational teams to handle cybercrime**

Legislation / Policy Framework

- Enact/Domesticate appropriate ECOWAS Community Acts
- Accede and Ratify relevant regional and international texts
- **Elaborate a regional policy on Critical Information Infrastructure Protection**

Resilience

- **Establish Computer Emergency Response Teams (CERTs)**
- **Critical Information Infrastructure Protection**
- Implement Public Key Infrastructure (PKI)
- Establish a Regional Cyber Security Centre

Capacity Building

- Build a critical mass of cyber work force
- **Awareness and Sensitisation campaigns**
- **Promote digital hygiene**

International Cooperation

- Facilitate the procedure to secure electronic evidence
- Facilitate cooperation to handle cybercrime



ECOWAS COMMISSION
COMMISSION DE LA CEDEAO
COMISSÃO DA CEDEAO

C. Current Situation



ECOWAS COMMISSION
COMMISSION DE LA CEDEAO
COMISSÃO DA CEDEAO

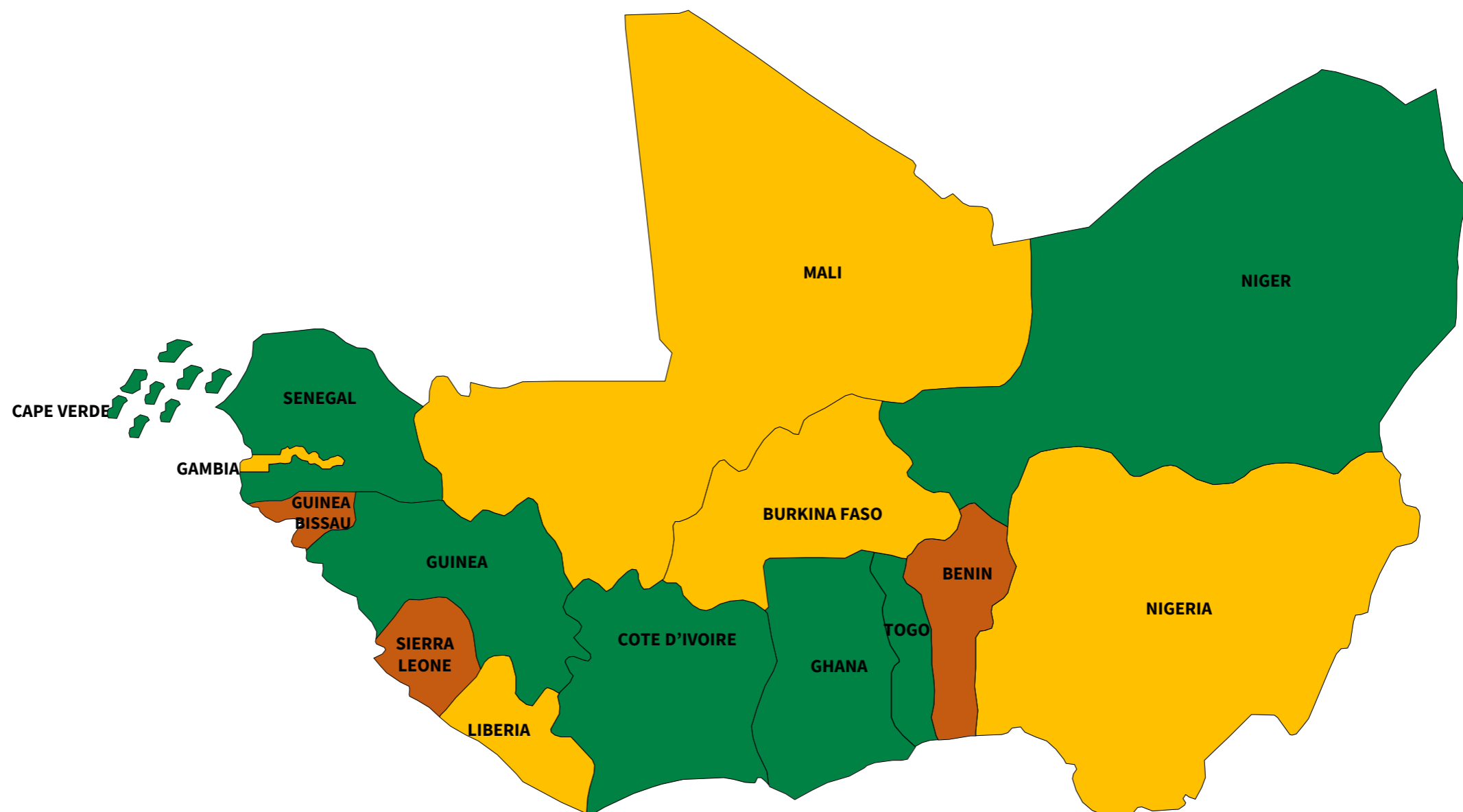
National Cybersecurity Strategy





ECOWAS COMMISSION
COMMISSION DE LA CEDEAO
COMISSÃO DA CEDEAO

African Union Convention on Cybersecurity and Data Protection (Malabo Convention)

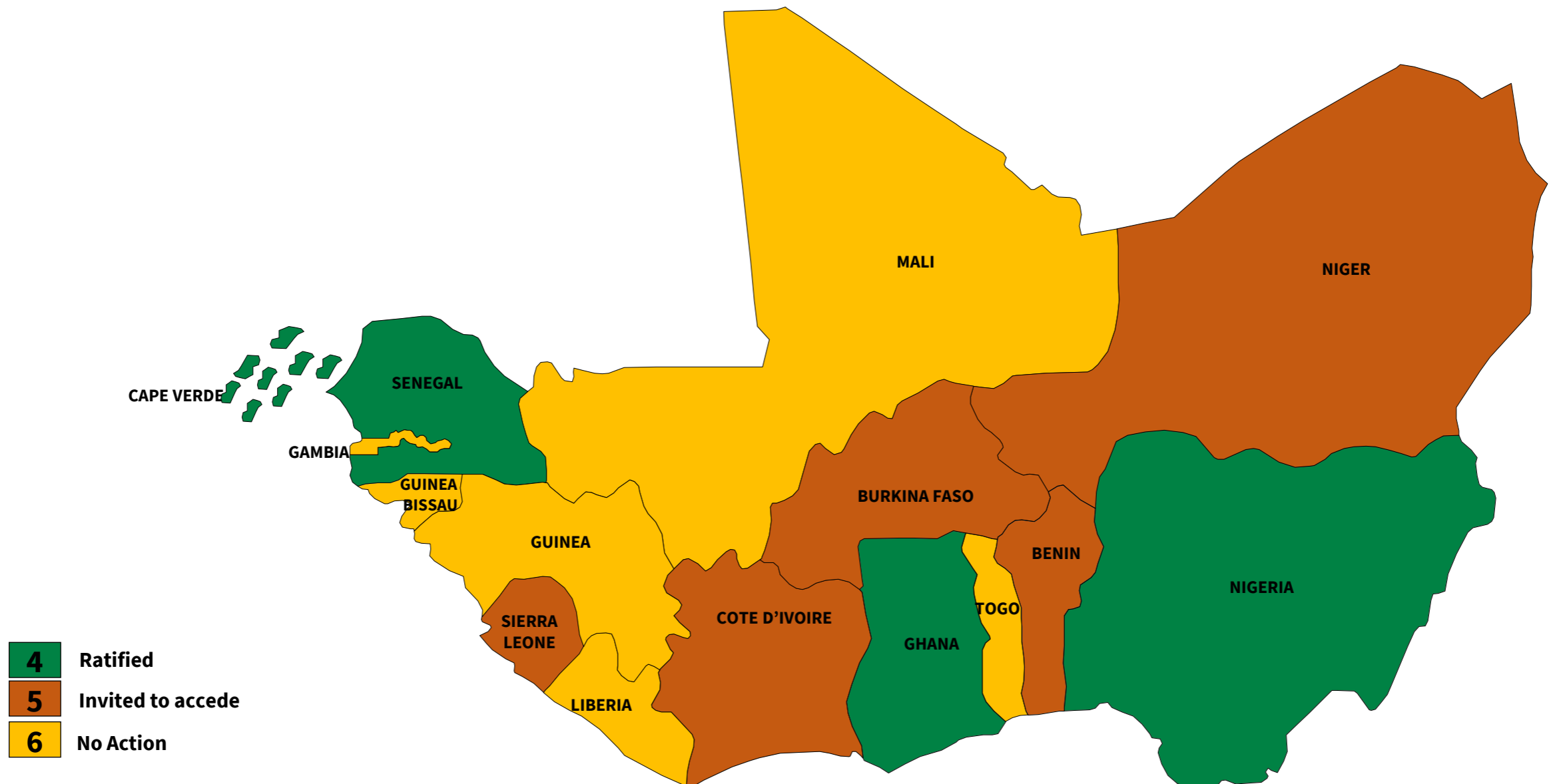


- 7** Ratified
- 3** Signed
- 5** No Action



ECOWAS COMMISSION
COMMISSION DE LA CEDEAO
COMISSÃO DA CEDEAO

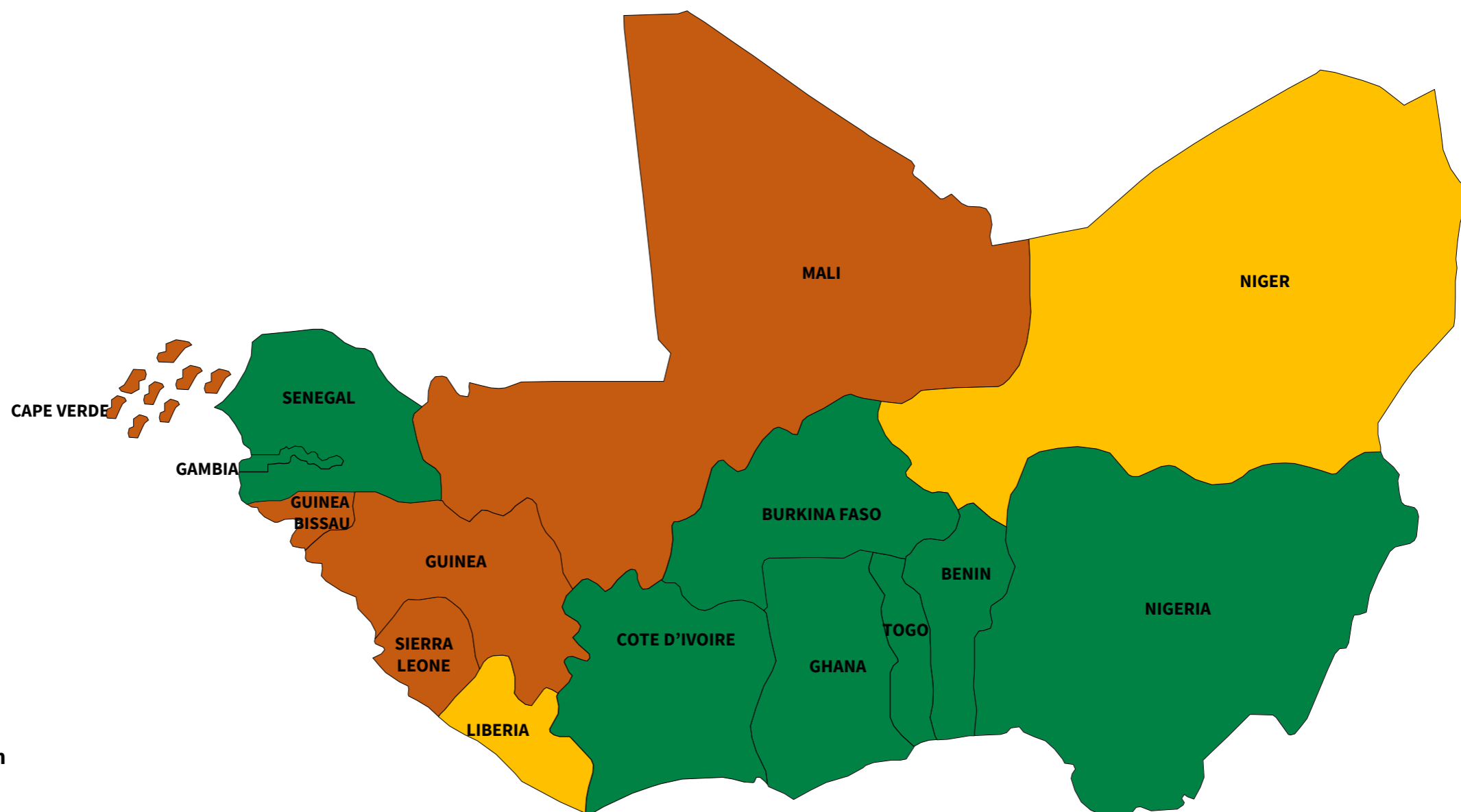
Convention on Cybercrime 185 (Budapest)





ECOWAS COMMISSION
COMMISSION DE LA CEDEAO
COMISSÃO DA CEDEAO

Computer Security Incident Response Teams



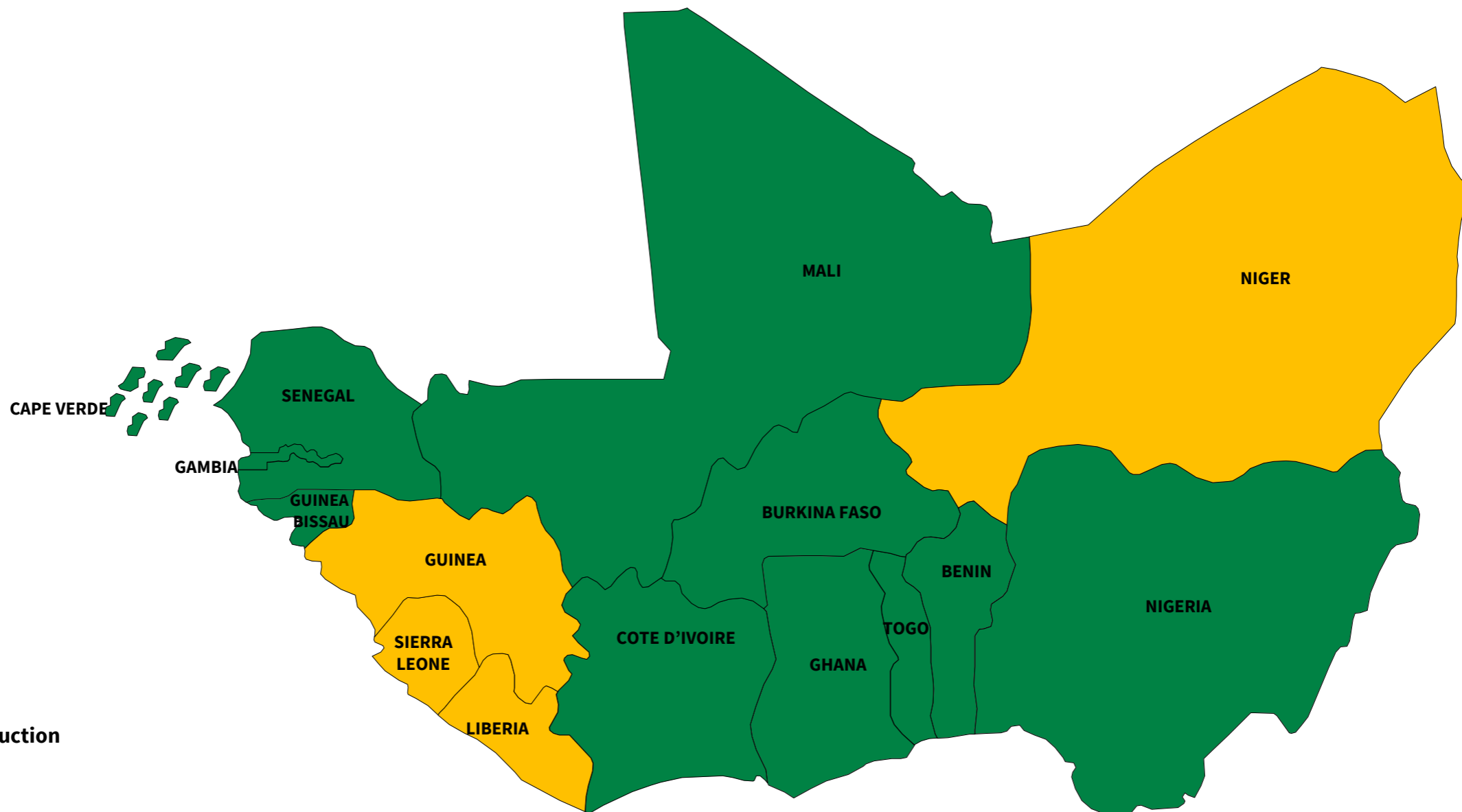
CSIRT

- 8 Available
- 5 Under Construction
- 2 None



ECOWAS COMMISSION
COMMISSION DE LA CEDEAO
COMISSÃO DA CEDEAO

Digital Forensic Laboratory



DFL

- 8** Available
- Under Construction**
- 7** None



ECOWAS COMMISSION
COMMISSION DE LA CEDEAO
COMISSÃO DA CEDEAO

Awareness

"Aie! Why did I share my PIN ?"



- Beware of phishing! Don't click on or open suspicious links or attachments.
- Surf safely. Only download from legitimate sites and be cautious of unsecured public wifi.
- Use strong passwords and passphrases, and change them regularly.
- Don't overshare personal information on social media.
- Install the latest security updates on your mobile phone or computer.



"I install updates, even at home."



- Beware of phishing! Don't click on or open suspicious links or attachments.
- Surf safely. Only download from legitimate sites and be cautious of unsecured public wifi.
- Use strong passwords and passphrases, and change them regularly.
- Don't overshare personal information on social media.
- Install the latest security updates on your mobile phone or computer.



"Is your home really secure ?"



- Beware of phishing! Don't click on or open suspicious links or attachments.
- Surf safely. Only download from legitimate sites and be cautious of unsecured public wifi.
- Use strong passwords and passphrases, and change them regularly.
- Don't overshare personal information on social media.
- Install the latest security updates on your mobile phone or computer.





Instruments

1. Regional Cybersecurity and Cybercrime Strategy
2. Regional Policy for the Protection of Critical Infrastructure



Forging ahead

Cyber diplomacy

West African cyber diplomats

Women in Cyber fellows
Sensitisation

Regional Confidence Building Measures (CBMs)

Cybercrime

Regional cyber coordination centre



7c's of Cyber

ⓘ Start presenting to display the poll results on this slide.



ECOWAS COMMISSION
COMMISSION DE LA CEDEAO
COMISSÃO DA CEDEAO

The 7c's of Cyber:

1. Collaboration
2. **Communication**
3. Cooperation
4. **Coordination**
5. **Commitment**
6. **Culture**
7. **Continuity**



Takeaways:

1. Garner Political will/commitment/influence to push cybersecurity to the top of national agendas.
2. Address gaps in legal & regulatory frameworks
3. Strengthen infrastructure inefficiencies
4. Fulfil obligation to strengthen capacity to build resilience
5. National buy in and ownership/commitment is important



ECOWAS COMMISSION
COMMISSION DE LA CEDEAO
COMISSÃO DA CEDEAO

Thank you

ECOWAS Commission
Directorate of Digital Economy & Post
folagunju@ecowas.int