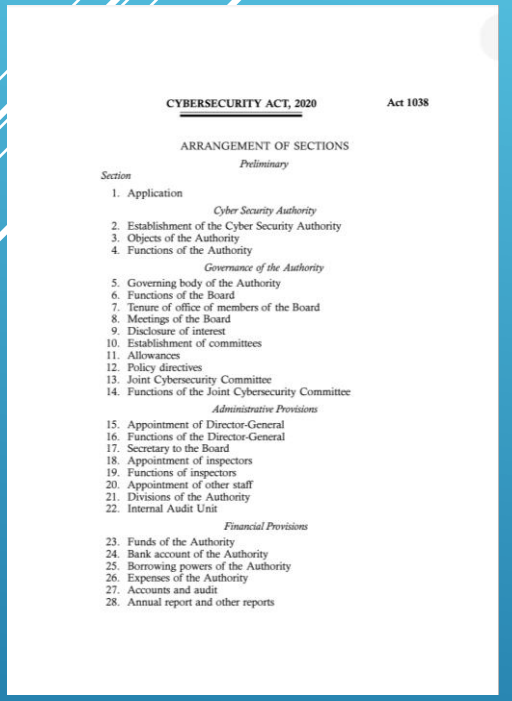
2021 COMMONWEALTH AFRICAN VIRTUAL CONFERENCE AND WORKSHOPS

Cyber Security

Legislation and Enforcement to Combat Cyber Threats:

Next Steps For Aligning National Cyber Legislation



CYBERSECURITY ACT, 2020 Act 1038

ARRANGEMENT OF SECTIONS

Preliminary

Section

1. Application

Cyber Security Authority

2. Establishment of the Cyber Security Authority
3. Objects of the Authority
4. Functions of the Authority

Governance of the Authority

5. Governing body of the Authority
6. Functions of the Board
7. Tenure of office of members of the Board
8. Meetings of the Board
9. Disclosure of interest
10. Establishment of committees
11. Allowances
12. Policy directives
13. Joint Cybersecurity Committee
14. Functions of the Joint Cybersecurity Committee

Administrative Provisions

15. Appointment of Director-General
16. Functions of the Director-General
17. Secretary to the Board
18. Appointment of inspectors
19. Functions of inspectors
20. Appointment of other staff
21. Divisions of the Authority
22. Internal Audit Unit

Financial Provisions

23. Funds of the Authority
24. Bank account of the Authority
25. Borrowing powers of the Authority
26. Expenses of the Authority
27. Accounts and audit
28. Annual report and other reports

OSEI BONSU DICKSON, BARRISTER
Chief Legal Advisor, Ministry of National Security
Government of Ghana
Chair, CyberX Africa Int'l Cyber Expo (20-22 Oct. 2022)

2021 COMMONWEALTH AFRICAN VIRTUAL CONFERENCE AND WORKSHOPS

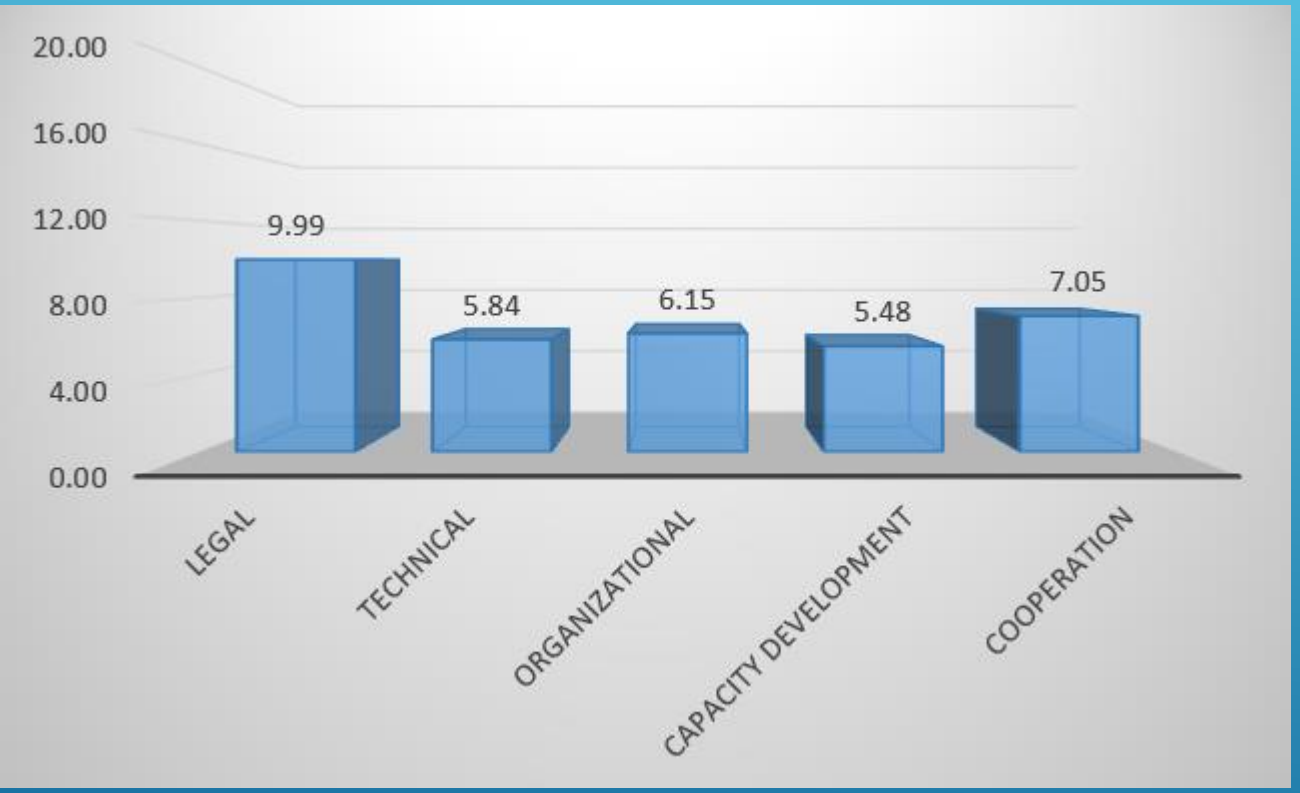
SPEAKER

OSEI BONSU DICKSON, BARRISTER

Expert, Cyber Security Law & Strategy in Africa

email: obdickson@gmail.com

Comparative Legislation- Africa



SOURCE - https://www.itu.int/en/myitu/News/2021/09/01/06/54/Are-African-countries-doing-enough-to-ensure-cybersecurity-and-Internet-safety

Towards the end of 2020 the ITU (Global Cyber Security Index) examined 194 countries to assess their commitment to improving cybersecurity based on five pillars: legal, technical, organizational, capacity development, and cooperation. The table is the overall performance of African countries.

Legal: Out of 54 African countries assessed, 29 had passed legislation to promote cybersecurity. 4 are at the stage of drafting policies or seeking legislative approval.

Africa comes second to Europe in terms of the prevalence of legislation. Of all the pillars assessed, this was the measure where Africa recorded its best performance.

LEGISLATION IN AFRICA: What do cybersecurity instruments in Africa cover – Lessons from West, East, North, and Southern Africa.

- **Matters with a focus on:**
  - Cyber criminal activity
  - Framework for cyber governance
  - Law enforcement and prosecution
  - International cooperation

OSEI BONSU DICKSON, ESQ, Ministry of National Security

CYBERX AFRICA

LEGISLATION IN AFRICA: Ghana, Kenya, Morocco, and Botswana.

GHANA, WEST AFRICA

In 2020, Ghana's Parliament passed the Countries Cyber Security Act, 2020 (Act 1038)

KENYA, EAST AFRICA

Kenya's Computer Misuse and Cybercrimes Act came into force on 30 May 2018. The Act protects computer systems, programs and data as well as facilitate detection, investigation, prosecution of cybercrimes.

MOROCCO, NORTH AFRICA

In November 2003, Morocco adopted Law No. 07-03, to govern attacks on automated data processing systems.

BOTSWANA. SOUTHERN AFRICA

Botswana's Cyber crime and Computer Related Crimes Act (No. 22 of 2007)

CYBERX AFRICA

LEGISLATION: Issues receiving the most legislative attention in Africa include :

- Legislation criminalizing specific malicious behaviors
- Legislation requiring Gov't agencies to implement cyber training
- Legislation requiring agencies to set up security policies, standards and practices, and to plan for and test how to respond to a security incidence.
- Legislation requiring CII designation and SOC/CERT in CIIs
- Legislation developing frameworks for coordinated response

CYBERX AFRICA

ENFORCEMENT: The major deliverables of many African legislations, include:

- Strengthening the Framework for Cyber Governance
- Strengthening Cyber Security, Intel and Threat Assessment
- Strengthening Operational Capacity
- Increasing Cyber Domain Awareness
- Strengthening Cyber Enforcement Regime

ENFORCEMENT: Challenges

Jurisdiction

One of the hurdles is Jurisdiction. Often investigators would realize that the perpetrator is outside their country or the legal jurisdiction of their courts. Which is why States are now focused on the international stage, using MLAs and establishing allies in the cyber world.

ENFORCEMENT: Challenges

Many cybercrimes go unreported

Majority of cyber-crimes do not get prosecuted because they are unreported to authorities. Many organizations fail to disclose breaches because of the negative impact and loss of trust that arises.

ENFORCEMENT: Challenges

Cyber-criminals are using advanced tools to cover their tracks.

Use of TOR and VPNs allows hackers to operate with a certain degree of anonymity. Beyond this, hackers work tirelessly to cover their tracks. Cyber-criminals are on the cutting edge of research, and they continuously work to evade identification, tracking, and apprehension.

ENFORCEMENT: Challenges

Digital Evidence collection is challenging.

Digital forensics has evolved. Best practices and strict processes have been developed to identify and preserve evidence to aid successful prosecution of cyber-criminals.

In many States however it is still challenging to prosecute cyber-criminals because few professionals have the expertise needed to gather and preserve admissible evidence.

ALIGNING LAW AND ENFORCEMENT IN AFRICA: Adoption of legislation should go hand-in-hand with the following next steps:

1. IMPROVEMENT in criminal justice capacities
2. ESTABLISHMENT of specialized units for cybercrime investigations
3. IMPROVING national computer forensic infrastructure
4. STRENGTHENING of law enforcement capacity, PPP and international cooperation
5. MAINSTREAMING cyber training into the CJS curricular

CYBERX AFRICA

QUO VADIS – AFTER LEGISLATION, WHAT IS NEXT FOR AFRICAN STATES?

Increase legal awareness to encourage behavioral change, such as preventive measures.

Invest in building up cybersecurity enforcement capabilities and technologies to detect and mitigate cybercrime.

Devote resources to setting up and equipping CERTs, ensuring adequate capacity to monitor and respond to incident reports.

Legislate efficient procedures for investigating and prosecuting cybercrime, thereby to deter cybercriminals.

Commit to enforcing cyber legislation while protecting digital rights.

CYBERX AFRICA

QUO VADIS – AFTER LEGISLATION, WHAT IS NEXT FOR AFRICAN STATES?

Where cybersecurity strategies are already in place, ensure better coordination and thus effective lawful implementation.

Strengthen legal partnerships between domestic stakeholders – public and private – to encourage the sharing of intelligence on potential threats and collaboration to find lasting solutions.

Enhance regional legal cooperation among African states to ensure a united voice when negotiating over multilateral cybersecurity standards.

Adopt a collective, region-wide approach that encourages peer learning and legal knowledge exchange.

CYBERX AFRICA

2021 COMMONWEALTH AFRICAN VIRTUAL CONFERENCE AND WORKSHOPS

Thank you

Any questions please ?

CSDS AFRICA