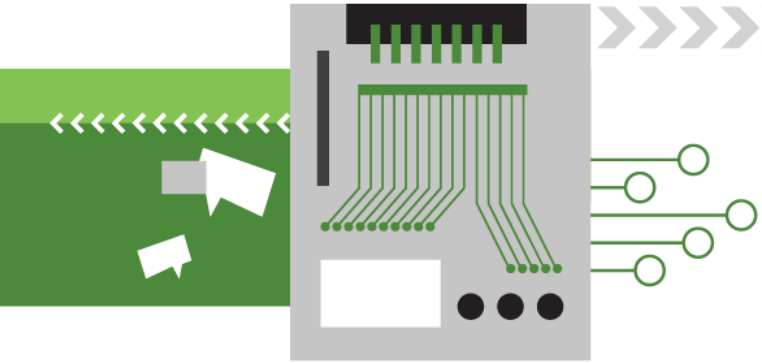


ENDCODE

TECH. LAW. POLICY. AFRICA

AUCC: OVERVIEW AND STATUS

PRIA CHETTY/ENDCODER

CONTENT

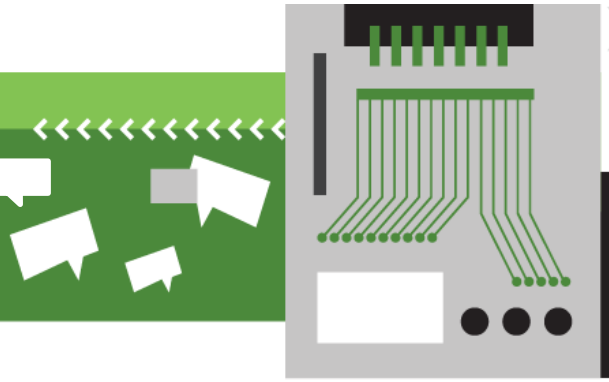
INTRODUCTION TO AUCC

ELECTRONIC COMMERCE

PROTECTION OF PERSONAL DATA

CYBERSECURITY

IMPLEMENTATION AND STATUS



CYBERSECURITY CHALLENGE IN AFRICA

Internet Blackouts, Elections Increasingly Linked in African Countries

WASHINGTON — It's becoming commonplace in many African nations: as an election approaches, the internet goes dark. Gabon is the latest country to employ internet censorship during a closely contested election, but other countries, including Uganda, Burundi, Ethiopia, Chad, Mali, Zimbabwe and the Republic of Congo have used the tactic this year, either during elections or in response to protests.

Observers say that as internet access becomes a necessity in the lives of many people, a dialogue is needed on how to balance security and openness. Right now, many countries simply opt for an information blackout when faced with unrest.

The organization Access Now, an advocacy group studying global digital risks, reported that there have been 40 widespread Internet disruptions in 25 countries this year alone.

"In the African context, where do you separate democracy and security?" asked Kamissa Camara, a West and Central Africa political analyst at the National Endowment for Democracy, in an interview with VOA Afrique.

"Is security more important than democracy? Do you place it above democracy? And who decides that the fact that young people use social networks threatens security in the country? These are the big questions to which I don't have an answer."

As the election approaches, the internet goes dark in African countries

Need to achieve a balance security and openness

40 widespread internet disruptions in 25 countries

http://www.voanews.com/a/internet-blackouts-elections-increasingly-linked-in-african-countries/3520704.html

INTERNET OF THINGS

13 AUG 2015

HOW THE INTERNET OF THINGS IS HAVING AN IMPACT IN AFRICA

The Internet of Things has already made an impact on Africa as the emergence of connected hardware takes off. Every area of life stands to benefit from the innovations and efficiencies possible in a fully connected world.

"The IoT is a reality that cannot be ignored," says Matthew Blewett, Chief Investment Officer at Business Connexion. "It's changing the way companies operate, forcing them to redefine their business processes to keep up with their competitors."

Furthermore, it will force many businesses to completely redefine their traditional value chains. "By making traditionally physical and disconnected processes digital and connected, products and services can be processed and delivered in completely new ways. This means that traditional value chains are being totally redefined."

Andy Brauer, Chief Technology Officer at Business Connexion cites Uber as a good example of a business that recognised how an IoT world allowed them to offer a service in a completely new and optimised way. "Uber saw the gap in the personal public transport space. In a connected world with mobile applications, geo-location and GPS

Connected Hardware

Innovations Efficiencies

Personal data protection for location data?

How to embed security in new business processes?

Photo: The Observer

Government offers free internet from 6pm to 6am in Kampala and Entebbe.

By Sadab Kitatta Kaaya

Government's offer of free Wi-Fi in Kampala and Entebbe has drawn strong opposition from some civil society activists.

The project, which started on October 1, is being implemented through the National Information and Technology Authority - Uganda (NITA-U). The activists believe it might be a deceptive manoeuvre to spy on the public, especially government critics.

In installing the free Wi-Fi hotspots (#MYUG), the government said it intends to broaden the reach of internet access to the public. However, obtaining Wi-Fi access requires users to first register their particulars such as name, date of birth, gender, phone and email contacts. This prerequisite has raised suspicions within the civil society community.

Free Wi-Fi in Kampala opposed as internet surveillance by government.

Internet access required registration and identification: gender, phone and email contacts.

http://allafrica.com/stories/201610120309.html

Of the 11 European countries that identified criminal suspects and/or infrastructure (CSI) in 13 different African states throughout 2015/2016, Nigeria featured as a cybercrime hotspot for all of them, according to the latest Europol Internet Organised Crime Threat Assessment (IOCTA) 2016 report.

Europol is the European Union's (EU) law enforcement agency established to assist EU Member States in their fight against serious international crime and terrorism, including cybercrime.

Europol Director Rob Wainwright says IOCTA 2016 provides a predominantly law enforcement focused assessment of the key developments, changes and emerging threats in the field of cybercrime over the last year.

In its brief summary of geographic threats and cybercrime activity throughout 2015-2016, based on law enforcement and industry data, Nigeria emerged as the third most frequently identified country as the location for CSI alongside the United Kingdom and Germany.

Though the report did not reflect the number of individual investigations, it says Africa still has the lowest global internet penetration (28.6%) although the continent boasts of a rapidly growing internet infrastructure and covers 10% of global internet users (compared to Europe, which has 17% despite 74% penetration) .

READ MORE

Nigeria tackles exploitation of its cyberspace
Ground patrol means everything in Africa's IT security
Interpol arrest sheds light on cybercriminal network
EU

Africa now suffers more from power distribution issues than internet access (having benefited from a series of high bandwidth undersea conduits along the eastern and western seaboards) and many states are rapidly adopting cybercrime legislation. However, they continue to lag behind when it comes to implementing and practising cyber security.

It also notes that Africa now has one of the highest global mobile malware infection rates. This is as a consequence of some African nations having profited "from being able to skip a number of technology milestones such as landlines and branch banking, instead leaping straight to mobile telephones and online banking."

Nigeria identified as a cybercrime hotspot by Europol

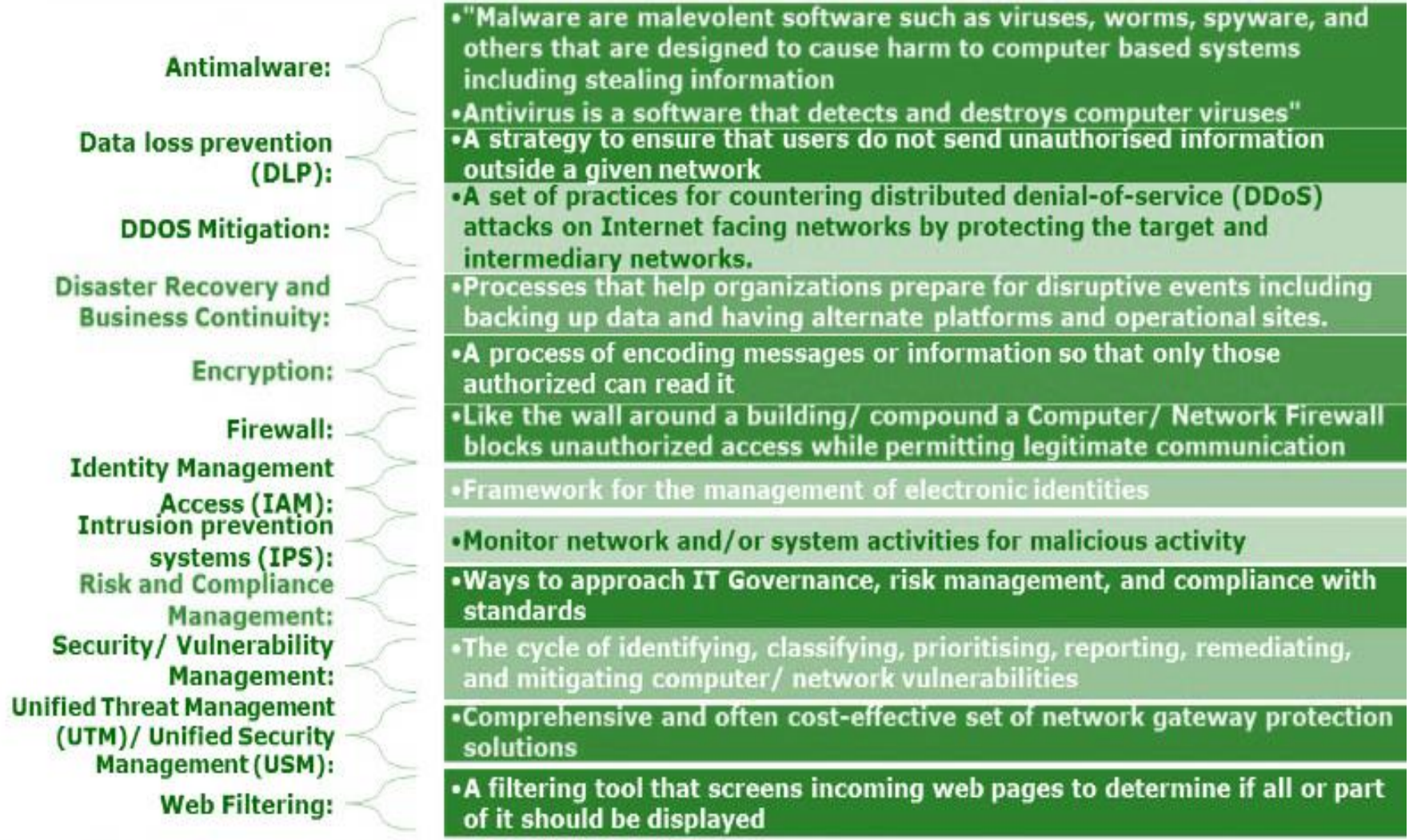
Third most frequently identified country as the location for criminal suspects or infrastructure alongside the UK and Germany

Many states are rapidly adopting cybercrime legislation.

Highest global malware infection.

http://www.itwebafrica.com/security/513-africa/236869-europol-identifies-nigeria-as-a-cybercrime-hotspot

AFRICA CYBER SECURITY MARKET WORTH $0.92 BILLION IN 2015 & **$2.32 BILLION BY 2020**



Source: http://www.marketsandmarkets.com/PressReleases/africa-cyber-security.asp

Abdul-Hakeem Ajijola (.AhA) info@consultancyss.com

CYBERSECURITY IN AFRICA

- Mechanisms of cooperation across national borders in Africa to solve and prosecute cybercrimes are complex and slow.

- Cyber criminals can *defy the conventional jurisdictional realms of sovereign nations*, originating an attack from almost any computer in the world, passing it across multiple national boundaries, or designing attacks that appear to be originating from foreign sources. Such techniques *dramatically increase both the technical and legal complexities of investigating and prosecuting cybercrime*s.

- Cybercrime has increased in increased in sophistication and frequency likely aligned to infrastructural, legal and policy loopholes in the countries with weaker responses.

- Cybercrime also poses *threat to the economic opportunities for the continent as a whole*.

- *National governments must grow their information security ranking through: an assessment of the strength of legal protections and progress for electronic transactions and data protection and to prosecute cyber criminals. A predictable environment with effective deterrence for computer crime is critical to competitiveness for countries that are growing their knowledge economy readiness. Africa is no exception.*

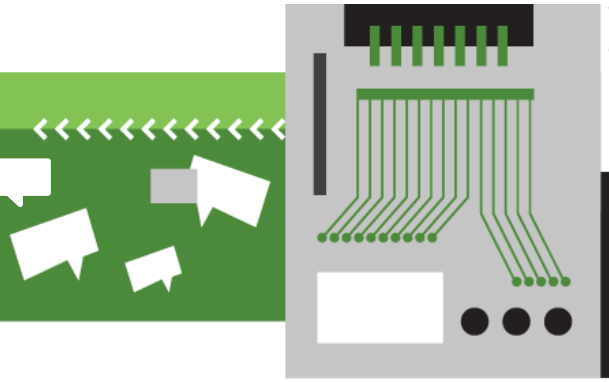
CYBERSECURITY GOVERNANCE

- UNCITRAL
- Budapest Conv.
- EU
- ITU
- UNCTAD
- UNECA
- AU
- SADC
- EAC
- ECOWAS
- *Others: OECD, WIPO*
- National

Globally, there are multiple initiatives, efforts, models at international, national and regional levels. Particularly to:

Promote harmonised, global, coherent and co-ordinated approaches;
Address legal barriers to electronic transactions; and
Promote trust and confidence in (international) electronic transacting methods

ENDCODE
Tech. Law. Policy. Africa.



INTRODUCTION TO AUCC

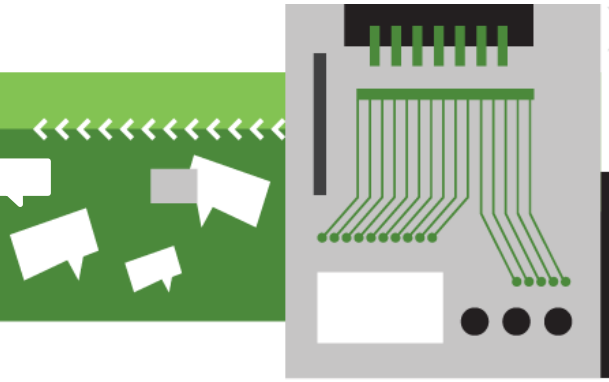
AUCC

- The African Union Cybersecurity Convention and Personal Data Protection (AUCC/ Convention) was adopted at the 23rd Ordinary Session of the Assembly of the Union, Malabo, on the 27th June 2014.

- *Establishes a Legal Framework for Cyber-security and Personal Data Protection that embodies the existing commitments of African Union Member States at sub- regional, regional and international levels to build the Information Society and address the need for harmonized legislation in the area of cyber security in Member States of the African Union*.

- Responds to the current state of cybercrime which constitutes a real threat to the security of computer networks and the development of the Information Society in Africa. In this regard it seeks to define broad guidelines of the strategy for the repression of cybercrime in African Union and to establish in each State party mechanisms for combating cybercrime.

- Acknowledges that violations of privacy may be generated by personal data collection, processing, transmission, storage and use.
- Open to all Member States of the Union, for signature and ratification.



CHAPTER I: ELECTRONIC COMMERCE

ARTICLE 2: SCOPE OF APPLICATION OF ELECTRONIC COMMERCE

1. (Subject to exceptions) Member States shall ensure that e-commerce activities shall be exercised freely in all State Parties ratifying or acceding to this Convention.

2. Without prejudice to other information obligations defined by extant legislative and regulatory texts in African Union Member States, State Parties shall ensure that any person exercising e-commerce activities shall provide to those for whom the goods and services are meant, easy, direct and uninterrupted access using non-proprietary standards with regard to specified information.

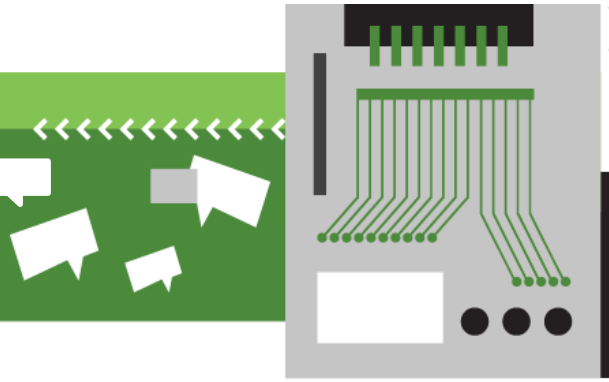
- Article 3: Contractual liability of the provider of goods and services by electronic means
- Article 4: Advertising by electronic means
- Article 5: Electronic contracts
- Article 6: Writing in electronic form

ARTICLE 7: ENSURING THE SECURITY OF ELECTRONIC TRANSACTIONS

1. The supplier of goods shall allow his/her clients to **make payments using electronic payment methods approved by the State according to the regulations in force in each State Party**. The supplier of goods or provider of services by electronic means who claims the discharge of an obligation must prove its existence or otherwise prove that the obligation was discharged or did not exist.

3. **A copy or any other reproduction of contracts signed by electronic means shall have the same probative value as the contract itself**, where the said copy has been certified as a true copy of the said act by bodies duly accredited by an authority of the State Party.
b) Certification will result in the issuance, where necessary, of a certificate of conformity.

4. **An electronic signature created by a secure device which the signatory is able to keep under his exclusive control and is appended to a digital certificate shall be admissible as signature on the same terms as a handwritten signature**. The reliability of the procedure is presumed, unless otherwise proven, if the electronic signature is generated by a secure signature creation device, the integrity of the act is guaranteed and the identification of the signatory is ensured.



CHAPTER II: PERSONAL DATA PROTECTION

ARTICLE 8: OBJECTIVE OF THIS CONVENTION WITH RESPECT TO PERSONAL DATA

1. Each State Party shall commit itself to establishing a legal framework aimed at strengthening fundamental rights and public freedoms, particularly the protection of physical data, and punish any violation of privacy without prejudice to the principle of free flow of personal data.

2. The mechanism so established shall ensure that any form of data processing respects the fundamental freedoms and rights of natural persons while recognizing the prerogatives of the State, the rights of local communities and the purposes for which the businesses were established.

ARTICLE 11: STATUS, COMPOSITION AND ORGANIZATION OF NATIONAL PERSONAL DATA PROTECTION AUTHORITIES

- Each State Party shall establish an authority in charge of protecting personal data.
- The national protection authority shall be an independent administrative authority with the task of ensuring that the processing of personal data is conducted in accordance with the provisions of this Convention.
- Each national protection authority shall formulate rules of procedure containing, inter alia, rules governing deliberations, processing and presentation of cases.

- State Parties shall undertake to provide the national protection authority with the human, technical and financial resources necessary to accomplish their mission.

ARTICLE 13: BASIC PRINCIPLES GOVERNING THE PROCESSING OF PERSONAL DATA

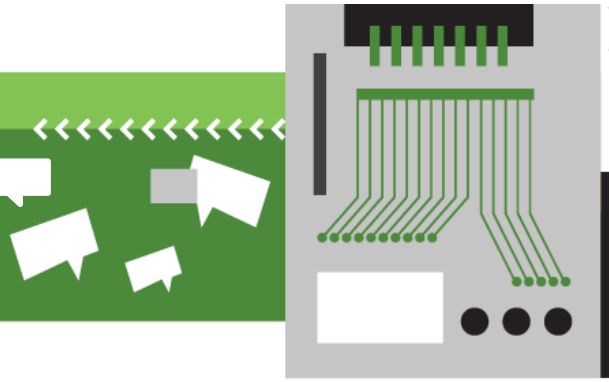
- Principle 1: Principle of **consent and legitimacy of personal data processing**
- Principle 2: Principle of **lawfulness and fairness of personal data processing**
- Principle 3: Principle of **purpose, relevance and storage of processed personal Data**
- Principle 4: Principle of **accuracy of personal data**
- Principle 5: Principle of **transparency of personal data processing**
- Principle 6: Principle of **confidentiality and security of personal data processing**

SECTION IV: THE DATA SUBJECTS' RIGHTS

- Article 16: **Right to information**
- Article 17: **Right of access**
- Article 18: **Right to object**
- Article 19: **Right of rectification or erasure**

SECTION V: OBLIGATIONS OF THE PERSONAL DATA CONTROLLER

- Article 20: **Confidentiality obligations**
- Article 21: **Security obligations**
- Article 22: **Storage obligations**
- Article 23: **Sustainability obligations**



CHAPTER III: PROMOTING CYBER SECURITY AND COMBATING CYBERCRIME

ARTICLE 24: NATIONAL CYBER SECURITY FRAMEWORK

1. National policy

Each State Party shall undertake to develop, in collaboration with stakeholders, a national cyber security policy which recognizes the importance of Critical Information Infrastructure (CII) for the nation identifies the risks facing the nation in using the all hazards approach and outlines how the objectives of such policy are to be achieved.

2. National strategy

State Parties shall adopt the strategies they deem appropriate and adequate to implement the national cyber security policy, particularly in the area of legislative reform and development, sensitization and capacity-building, public-private partnership, and international cooperation, among other things. Such strategies shall define organizational structures, set objectives and timeframes for successful implementation of the cyber security policy and lay the foundation for effective management of cyber security incidents and international cooperation.

ARTICLE 25: LEGAL MEASURES

1. Legislation against cybercrime: Each State Party shall adopt such legislative and/or regulatory measures as it deems effective by considering as substantive criminal offences acts which affect the confidentiality, integrity, availability and survival of information and communication technology systems, the data they process and the underlying network infrastructure, as well as effective procedural measures to pursue and prosecute offenders. State Parties shall take into consideration the choice of language that is used in international best practices.

2. National Regulatory Authorities: Each State Party shall adopt such legislative and/or regulatory measures as it deems necessary to confer specific responsibility on institutions, either newly established or pre-existing, as well as on the designated officials of the said institutions, with a view to conferring on them a statutory authority and legal capacity to act in all aspects of cyber security application, including but not limited to response to cyber security incidents, and coordination and cooperation in the field of restorative justice, forensic investigations, prosecution, etc.

3. Rights of citizens: In adopting legal measures each State Party shall ensure that the measures so adopted will not infringe on the rights of citizens guaranteed under the national constitution and internal laws, and protected by international conventions, particularly the African Charter on Human and Peoples‟ Rights, and other basic rights such as freedom of expression, the right to privacy and the right to a fair hearing, among others.

4. Protection of critical infrastructure: Each State Party shall adopt such legislative and/or regulatory measures as they deem necessary to identify the sectors regarded as sensitive for their national security and well-being of the economy, as well as the information and communication technologies systems designed to function in these sectors.

ARTICLE 26: NATIONAL CYBER SECURITY SYSTEM

- 1. Culture of Cyber Security
- 2. Role of Governments
- 3. Public-Private Partnership
- 4. Education and training

ARTICLE 27: NATIONAL CYBER SECURITY MONITORING STRUCTURES

1. Cyber security governance

a) Each State Party shall adopt the necessary measures to establish an appropriate institutional mechanism responsible for cyber security governance;
b) The measures adopted as per paragraph 1 of this Article shall establish strong leadership and commitment in the different aspects of cyber security institutions and relevant professional bodies of the State Party. To this end, State Parties shall take the necessary measures to:

i) Establish clear accountability in matters of cyber security at all levels of Government by defining the roles and responsibilities in precise terms;
ii) Express a clear, public and transparent commitment to cyber security;
iii) Encourage the private sector and solicit its commitment and participation in government-led initiatives to promote cyber security.

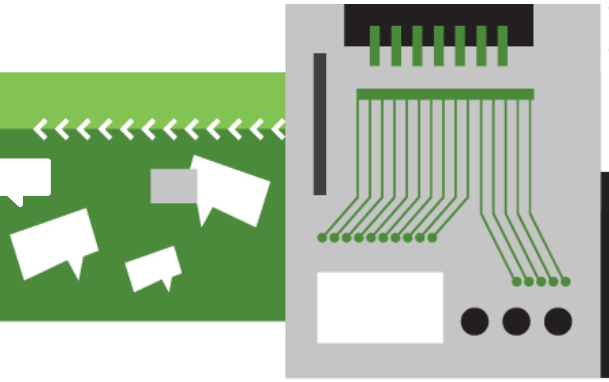
c) Cyber security governance should be established within a national framework that can respond to the perceived challenges and to all issues relating to information security at national level in as many areas of cyber security as possible.

ARTICLE 28: INTERNATIONAL COOPERATION

- 1. Harmonization
- 2. Mutual legal assistance
- 3. Exchange of information
- 4. Means of cooperation

ARTICLE 29: OFFENCES SPECIFIC TO INFORMATION AND COMMUNICATION TECHNOLOGIES

- 1. ATTACKS ON COMPUTER SYSTEMS
- 2. COMPUTERIZED DATA BREACHES
- 3. CONTENT RELATED OFFENCES
- 4. OFFENCES RELATING TO ELECTRONIC MESSAGE SECURITY MEASURES



CHAPTER IV: FINAL PROVISIONS

ARTICLE 32: MEASURES TO BE TAKEN AT THE LEVEL OF THE AFRICAN UNION

The Chairperson of the Commission shall report to the Assembly on the establishment and monitoring of the operational mechanism for this Convention. The monitoring mechanism to be established shall ensure the following (by way of example):

a) Promote and encourage the Continent to adopt and implement measures to strengthen cyber security in electronic services and in combatting cybercrime and human rights violations in cyberspace;
b) Gather documents and information on cyber security needs as well as on the nature and magnitude of cybercrime and human rights violations in cyberspace;
c) Work out methods for analysing cyber security needs, as well as the nature and magnitude of cybercrime and human rights violations in cyberspace, disseminate information and sensitize the public on the negative effects of these phenomena;

ARTICLE 35: SIGNATURE, RATIFICATION OR ACCESSION

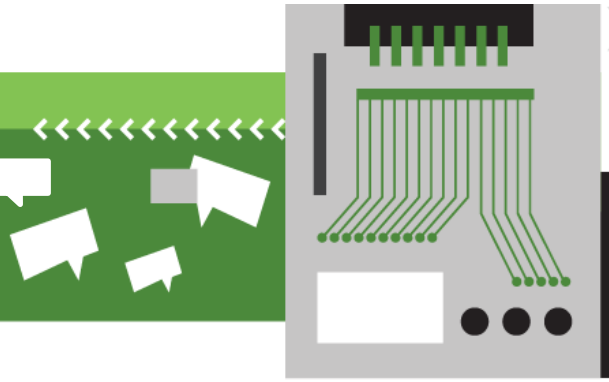
This Convention shall be open to all Member States of the Union, for signature, ratification or accession, in conformity with their respective constitutional procedures.

ARTICLE 36: ENTRY INTO FORCE

This Convention shall enter into force thirty (30) days after the date of the receipt by the Chairperson of the Commission of the African Union of the fifteenth (15th) instrument of ratification.

ARTICLE 37: AMENDMENT

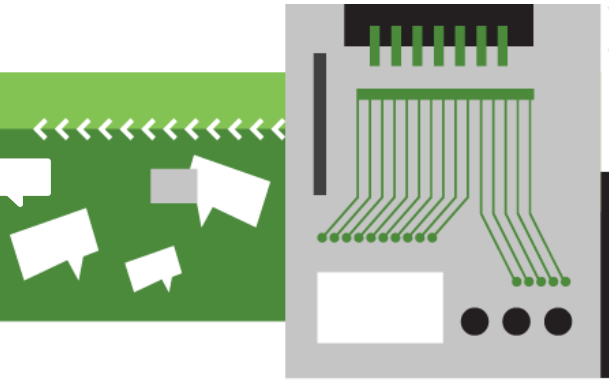
1. Any State Party may submit proposals for the amendment or revision of this Convention;
2. Proposals for amendment or revision shall be submitted to the Chairperson of the Commission of the African Union, who shall transmit same to State Parties within thirty (30) days of receipt thereof;



IMPLEMENTATION AND STATUS OF AUCC

SIGNATURE AND RATIFICATION STATUS

- 15 Ratifications required for entry into force
- Signatures: Benin, Chad,Congo, Ghana, Guinea Bissau, Mauritania, Sierra Leone, Sao Tome and Principe, and Zambia have signed the convention
- 2 Ratifications: (Sénégal 3/8/2016, Guinea 1/06/17)



SUMMARY OF OBLIGATIONS OF MEMBER STATES

POLICY AND GOVERNANCE MEASURES

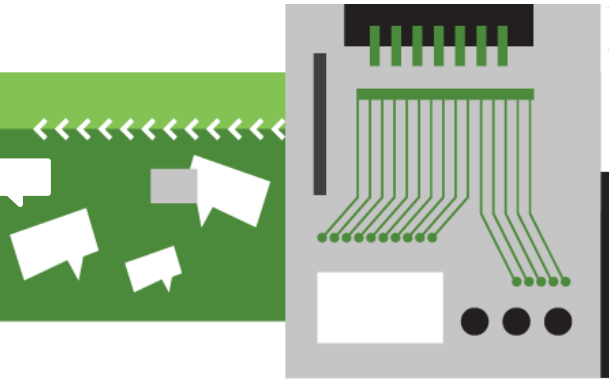
- Public private partnerships to engage industry, civil society, and academia in the promotion and enhancement of a cybersecurity culture
- Cybersecurity Policy which recognises the Critical Information Infrastructure and identifies the risks to the nation and mitigation measures
- National Cybersecurity strategy to implement the Policy

LEGISLATIVE AND REGULATORY MEASURES

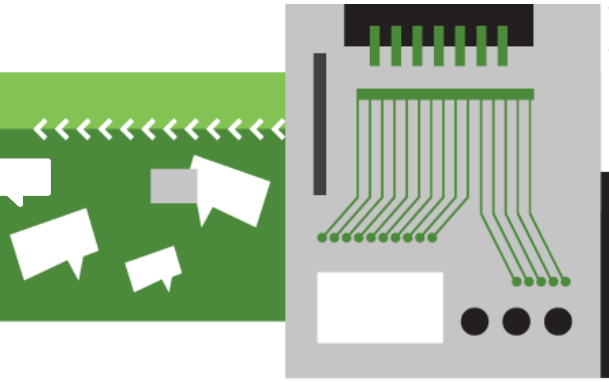
- Legislative and regulatory measures to *identify the sectors regarded as sensitive for their national security and well-being of the economy (critical infrastructure*), and measures to improve vigilance, security and management in such sectors
- Data Protection Laws and Regulations
- Electronic Commerce Laws and Regulations
- Cybercrime Laws and Regulations

INSTITUTIONAL MEASURES

- Institutions that *exchange information on cyber threats and vulnerability assessments* such as the Computer Emergency Response Teams (CERTs)
- State Department to *regulate and vulnerability and safety guarantee assessments of ICT product vendors* including ensuring mandatory disclosures of vulnerabilities and the solutions to such vendors consumers
- Institutions with the statutory *authority and legal capacity to respond to cyber security incidents*, co-ordination and co-operation for (cybersecurity) restorative justice, forensic investigations, cybersecurity prosecution
- Institutions responsible for *national and cross-border co-ordination of cybersecurity* problems as well as global co-operation
- *Data Protection Authority* whose responsibilities in regulating data protection include: authorisation of data processing, authorisation of cross border transfers of personal data
- Electronic Signature Accreditation A*uthority that will regulate what constitutes a qualified electronic signature* for the purposes of authenticating electronic records and other applications
- State Department to *regulate and approve electronic commerce payment methods*, only approved payment methods may be validly used in the Member State territory



WAY FORWARD



PRIA CHETTY/ENDCODER/

THANKS, QUESTIONS?

pria.chetty@endcode.org
endcode.org