AFRICA AND THE UN CYBERCRIME CONVENTION PROCESS

Prof. Nnenna Ifeanyi-Ajufo

15-04-2024

Organisation of the AHC

In December 2019, the UN General Assembly adopted a resolution on "countering the use of information and communications technologies for criminal purposes" and introducing an Ad Hoc Committee. In accordance with General Assembly resolution 75/282 and with General Assembly decision 76/552, the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, established by the General Assembly in its resolution 74/247.

The committee was announced to elaborate a comprehensive international convention. Thus, working towards creating a new international treaty on cybercrime.

Organisation of the AHC

Organizational session of the Ad Hoc Committee

NewYork, 10-12 May 2021

First session of the Ad Hoc Committee

28 February to 11 March 2022

Final Session NewYork, 29 January to 9 February 2023

In the first session 25 African countries out of the 55 AU member states

35 African countries in the Sixth Session

Africa's Involvement in the AHC

Compared to other processes that have focused on an international approach to ensure rule of law in cyberspace, the process leading to the elaboration of the AHC Process has seen quite commendable interest from the African Region.

At the inception, Africa displayed obvious interest in the Russia-China led UN Cybercrime process. Thirty-two (32) African countries voted in favour of the December 2018 Russia-backed resolution that required the UN Secretary-General to collect countries' views about cybercrime. About Thirty (30) African countries also voted in favour of the December 2019, Russia motivated UN General Assembly Resolution aimed to create the new cybercrime treaty United Nations General Assembly Resolution A/74/401 'Countering the use of information and communications technologies for criminal purposes' 25 November 2019.

COMPARATIVE ANALYSIS WITH OTHER PROCESSES

There was minimal African involvement in the United Nations process that resulted in the UN Norms of Responsible State Behaviour in Cyberspace. Since 2004, only nine African nations held membership in the UN Group of Governmental Experts (GGE). Notably, Egypt, Kenya and South Africa.

There was also no response from any African country for the 2020 Open Ended Working Group published Non-Paper Response of proposals and guidance on the UN CyberNorms.

United Nations mandated working group – the Open-Ended Working Group on 'Developments in the Field of ICTs in the Context of International Security' (OEWG) was established in parallel with the GGE, open to all interested states.

The AHC vs The Budapest

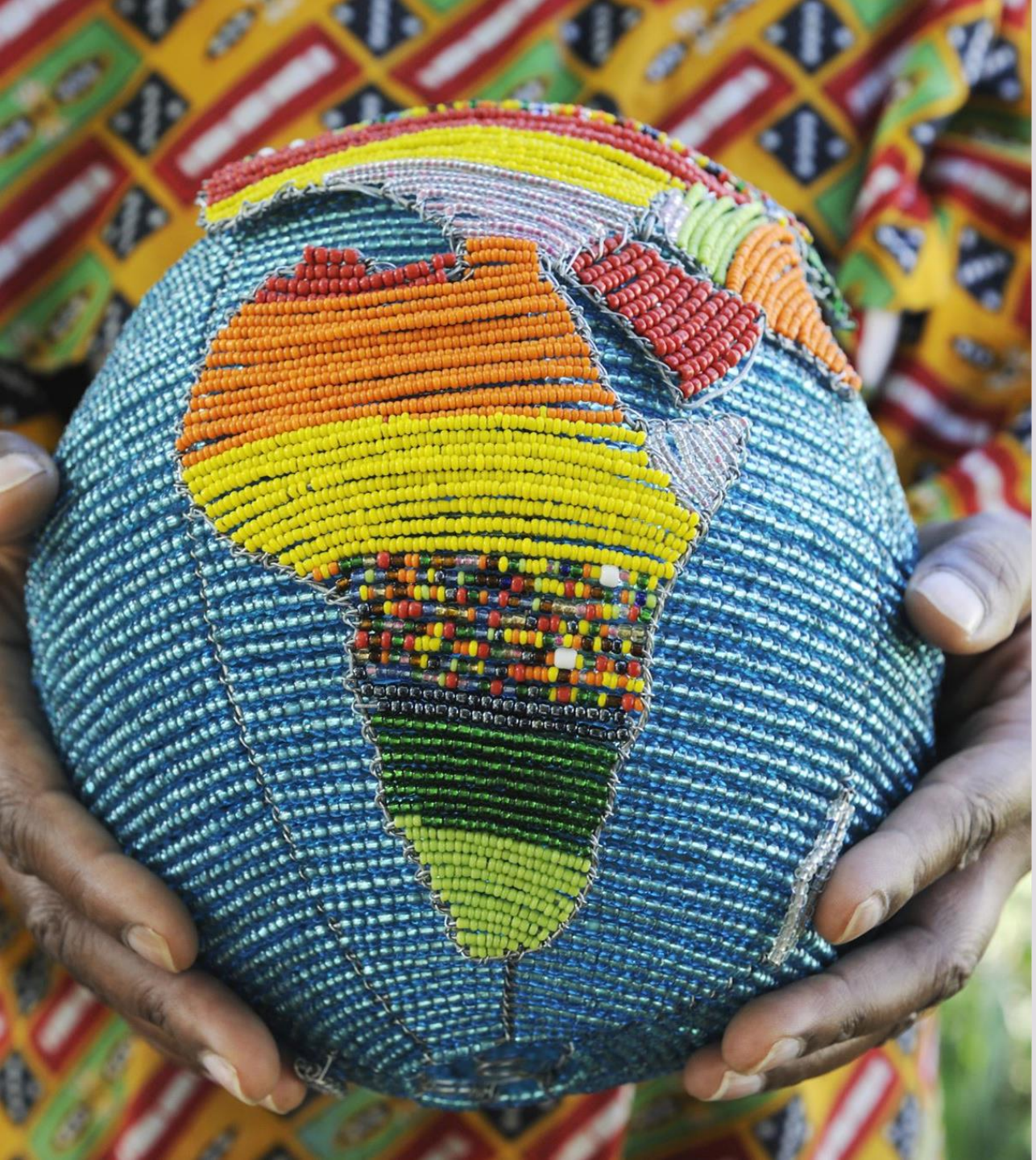
The difference between the UN Cybercrime process and the process that resulted in the Budapest Convention is that the UN Convention has allowed global involvement at the time of drafting unlike the limited regional involvement which the Budapest Convention represented at the time of drafting and so the UN Cybercrime Convention gives Africa an opportunity to be involved in the process on equal terms as other regions. Another incentive is that the UN Cybercrime process has been Chaired and Vice-Chaired by African Countries.

AFRICA'S LEADERSHIP COMPOSITION OF THE AHC

Chair- Algeria

Vice-Chair- Egypt

Vice-Chair - Nigeria



At the beginning of the AHC process, African countries present expressed confidence in the UN Cybercrime Convention towards fighting cybercrime especially because of the digital transformation pursuits of Africa, expressed in the Digital Transaformation Strategy 2020-2030, the ACFTA, the AU Agenda 2063 and what many states argued was the inadequacy of the African regional Cybersecurity Convention. Many states also hinged the priority being given to the UN Cybercrime process was because the interests of developing countries was expressed noting that “the purpose of the Convention is to promote and strengthen measures to prevent and combat cybersecurity, facilitate and enhance international cooperation and build capacity for cybersecurity particularly for developing countries,. - https://documents-dds-ny.un.org/doc/UNDOC/GEN/222/255/1E/PDF/2222551E.pdf?OpenElement

HOW THE CONVENTION FAVOURS AFRICA'S INTERESTS

INTERNATIONAL COOPERATION

TECHNICAL ASSISTANCE

CAPACITY BUILDING

PREAMBLE

"Stressing the need to enhance coordination and cooperation among States, including by providing technical assistance and capacity-building to countries, in particular developing countries, upon their request, to improve national legislation and frameworks and enhance the capacity of national authorities to deal with [cybercrime] [the use of information and communications technologies for criminal purposes] in all its forms, including its prevention, detection, investigation and prosecution, and emphasizing in this context the role that the United Nations plays…"

Statement of purpose

The purposes of this Convention are to: (a) Promote and strengthen measures to prevent and combat [cybercrime] [the use of information and communications technologies for criminal purposes] more efficiently and effectively; (b) Promote, facilitate and strengthen international cooperation in preventing and combating [cybercrime] [the use of information and communications technologies for criminal purposes]; and (c) Promote, facilitate and support technical assistance and capacity-building to prevent and combat [cybercrime] [the use of information and communications technologies for criminal purposes], in particular for the benefit of developing countries.

Chapter I General provisions Article 1 (proposed)

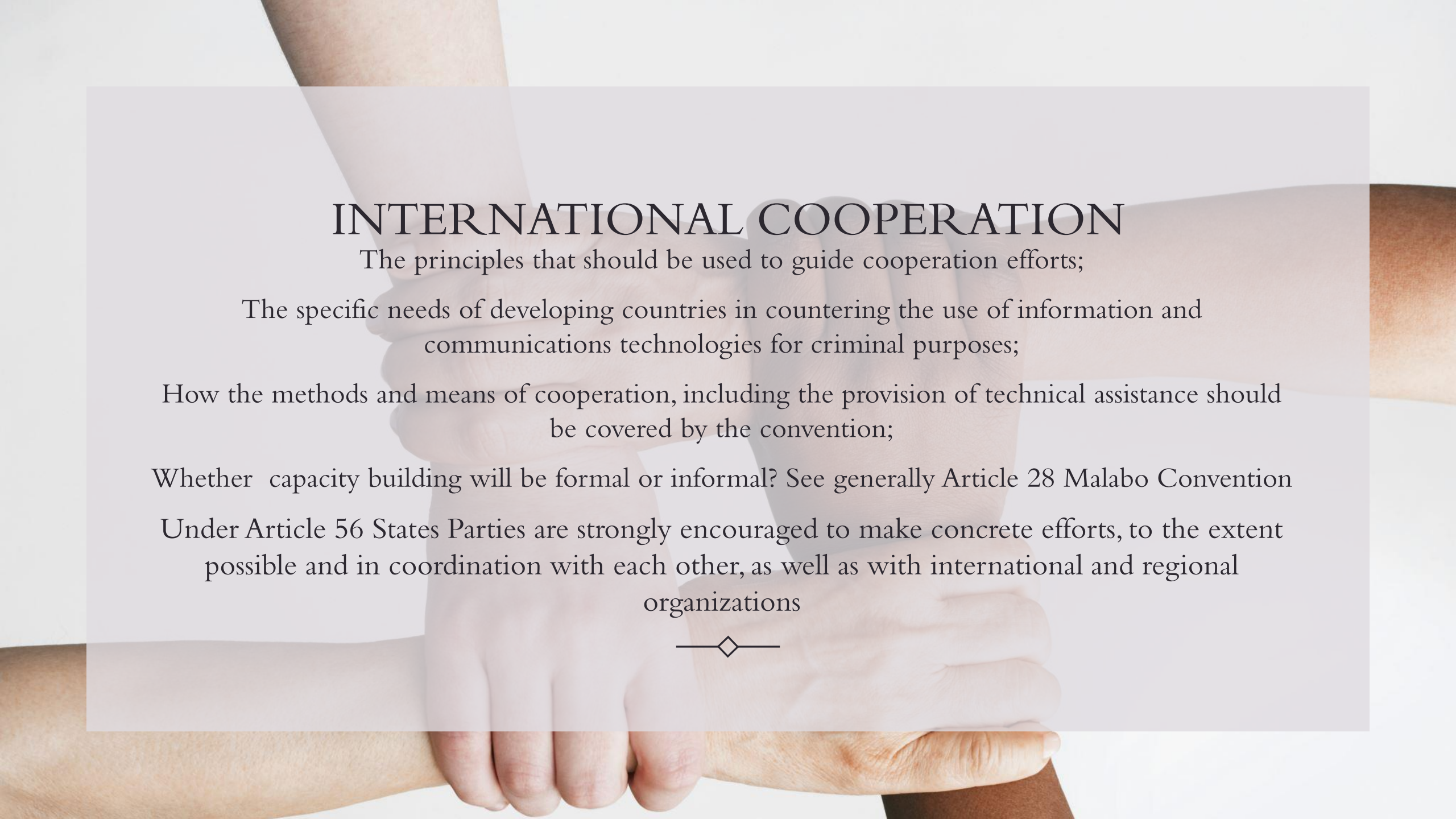
STATUS OF THE AFRICAN UNION IN THE AHC PROCESS

Representatives of global and regional intergovernmental organizations, including representatives of United Nations bodies, specialized agencies and funds, as well as representatives of functional commissions of the Economic and Social Council

AUC- MULTISTAKEHOLDER GROUP

African Union Cyber Security Experts Group (AUCSEG)

AFRICA GROUP



INTERNATIONAL COOPERATION

The principles that should be used to guide cooperation efforts;

The specific needs of developing countries in countering the use of information and communications technologies for criminal purposes;

How the methods and means of cooperation, including the provision of technical assistance should be covered by the convention;

Whether capacity building will be formal or informal? See generally Article 28 Malabo Convention

Under Article 56 States Parties are strongly encouraged to make concrete efforts, to the extent possible and in coordination with each other, as well as with international and regional organizations

INTERNATIONAL COOPERATION

Generally, States Parties are mandated to cooperate with each other in accordance with the provisions of this Convention, as well as other applicable international instruments on international cooperation in criminal matters, and domestic laws, for the purpose of investigations, prosecutions and judicial proceedings concerning offences in accordance with the Convention, or for the collection, obtaining, preservation and sharing of evidence in electronic form of offences established in accordance with the Convention

See Article 35 and Article 51 on Special cooperation

KEY CONCERNS FOR AFRICA?

Considering the articulation in regard to international cooperation, technical assistance, mutual legal assistance and data sharing, a huge question is whether Africa, will have the capacity to implement such a convention.

The Budapest Convention has obviously been a huge source of guidance for the submissions from the EU delegation and other EU States, how that is being interpreted by developing countries and whether their interests have also been given priority continues to be a debate. For example, similarity in texts.

Most developed countries for example, the European states already have systems of cooperation, resources, and capacity which provide adequate capability to address cybersecurity effectively

KEY CONCERNS FOR AFRICA?

For AFRICA, the definition of terms and scope of the convention may be an issue. Many African governments continue to voice concerns over hate speech, online terrorism, online defamation, disinformation and will certainly prefer a wider scope of criminalisation.

With the varied understandings of cybercrime and the varied objectives of tackling cybercrime Africa's interpretation of cybercrimes in their national legislations have been encompassing of and criminalises computer dependant and computer enabled crimes which the understanding that as long as such an activity bothers on the use of computers it is regarded as cybercriminal .Therefore, will a narrow scope of criminalisation be considered by African States as beneficial?

KEY CONCERNS FOR AFRICA?

Arguments related to international cooperation and its implications for Africa.

Questions as to how capacity building will continue to be interpreted on Africa's terms.

The process has prioritised exchange and sharing of data, particularly for evidentiary purposes. Many of the developed countries have existing and enforceable legislation to guide data sharing and data protection.

SOVEREIGNTY

Article 4 of the draft of the proposed convention generally protects sovereignty

States Parties shall carry out their obligations under this Convention in a manner consistent with the principles of sovereign equality and territorial integrity of State s and that of non-intervention in the domestic affairs of other States.

See Article 4

HUMAN RIGHTS

Articles 5&24. Human Rights and Conditions and safeguards- Each State Party shall ensure that the establishment, implementation and application of the powers and procedures are subject to conditions and safeguards provided for under its domestic law, which shall be consistent with its obligations under international human rights law, and which shall incorporate the principle of proportionality.

Article 15 - Conditions and safeguards 1 Each Party shall ensure that the establishment, implementation and application of powers and procedures provided are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.

Preventive measures- Cybersecurity culture

See generally Article 53 - Preventive measures may include: (a) Strengthening cooperation between law enforcement agencies or prosecutors and relevant stakeholders for the purpose of preventing and combating the offences covered by this Convention; (b) Promoting public awareness regarding the existence, causes and gravity of the threat posed by the offences covered by this Convention through public information activities, public education, media and information literacy programmes and curricula that promote public participation in preventing and combating such offences.

IN LINE WITH ARTICLE 26 MALABO CONVENTION

Articles 63&64

This Convention shall also be open for signature by regional economic integration organizations, provided that at least one member State of such an organization has signed the Convention

The Convention shall enter into force on the ninetieth day after the date of deposit of the fortieth instrument of ratification, acceptance, approval or accession. Any instrument deposited by a regional economic integration organization shall not be counted as additional to those deposited by member States of that organization.

FINAL SESSION – THOUGHTS?

01

Africa's understanding of cyber-diplomacy and the underlying implications of choices made.

02

The cooperation between public and private sector actors in the fight against cybercrime should be expanded on- 26(3) &27(1)(b)(iii)Malabo Convention

03

The new convention must be clear on what international cooperation measures and tools are available, especially for the digitally weaker states.

04

The new convention must include clear mechanisms of implementation.