Comparative analysis: Malabo Convention of African Union and Budapest Convention on Cybercrime

Zahid Jamil
Council of Europe Expert

Strasbourg 17 November 2016
Fundamentals of a Cybercrime Treaty

• **Global** instrument
  (Operational, Functional framework)

• Members:
  • should include **Infrastructure Countries**

• Definitions

• Offences

• Comprehensive procedural powers

• Comprehensive **Legally binding** International cooperation mechanism
BC

- **Global** instrument
- **Infrastructure Countries**
- **Cybercrime** and **electronic evidence** convention
- **Comprehensive procedural powers**
- **Functional international cooperation mechanism**

AUC

- **Regional** instrument
- **No Infrastructure Countries**
- **Cybercrime, cyber security, electronic transactions & data protection**
- **Missing key procedural powers**
- **No international cooperation mechanism**
Comprehensive

• Operational, Functional framework targeting:
  • cybercrime and
  • other criminal offences involving electronic evidence

• Provides for:
  • offences,
  • procedural powers and
  • international cooperation legally binding framework
Budapest Convention

• **Global** instrument

• Members – **Infrastructure Countries**

• Definitions

• Offences

• Comprehensive procedural powers

• Comprehensive **Legally binding** International cooperation mechanism
Scope of AU Convention

• **Deals with:**
  1. Electronic transactions,
  2. Personal Data Protection,
  3. Cyber security and
  4. Cybercrime

• AU Convention **political commitment on a range of issues including cybercrime**

• Attempt to **unite different IT Law aspects** and certain non-digital and non-criminal justice issues
• **Regional Instrument (No Infrastructure countries)**

• **Restricted to Cybercrime –not other offences**

• Definitions **missing** (e.g. procedural powers) foundational definitions are **vague** (e.g. computer system)

• Offences **not comprehensive** and are largely **missing mens rea elements**

• Many procedural powers are **missing**, rest are **vaguely** defined and **not** subject to **safeguards**

• **No international cooperation mechanism** (aspirational statements)
SUMMARY of FINDINGS
<table>
<thead>
<tr>
<th>Budapest Convention on Cybercrime (&quot;BC&quot;)</th>
<th>African Union Convention on Cyber Security and Personal Data Protection (&quot;AUC&quot;)</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Definitions</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Article 1.a &quot;computer system&quot;</td>
<td>Article 1. &quot;computer system&quot;</td>
<td>AUC different from BC</td>
</tr>
<tr>
<td>Article 1.b &quot;computer data&quot;</td>
<td>Article 1. &quot;computerized data&quot;</td>
<td>AUC incomplete but compatible with BC</td>
</tr>
<tr>
<td>Article 1.c &quot;service provider&quot;</td>
<td></td>
<td>Missing in AUC</td>
</tr>
<tr>
<td>Article 1.d &quot;traffic data&quot;</td>
<td></td>
<td>Missing in AUC</td>
</tr>
<tr>
<td>Protocol 189 Article 2 &quot;racist and xenophobic material&quot;</td>
<td>Article 1. &quot;racist and xenophobic material&quot;</td>
<td>AUC largely compatible with Protocol to BC</td>
</tr>
<tr>
<td>Article 18.3 &quot;subscriber information&quot;</td>
<td></td>
<td>Missing in AUC</td>
</tr>
<tr>
<td>Substantive criminal law</td>
<td>Article 29.1.a-c. Attacks on computer systems</td>
<td>AUC largely compatible with BC</td>
</tr>
<tr>
<td>-------------------------------------------------------------</td>
<td>-----------------------------------------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>Article 2. Illegal access</td>
<td>Article 29.2.a. Computerized data breaches</td>
<td>AUC largely compatible with BC</td>
</tr>
<tr>
<td>Article 3. Illegal interception</td>
<td>Article 29.1. e-f. Attacks on computer systems</td>
<td>AUC largely compatible with BC</td>
</tr>
<tr>
<td>Article 4. Data interference</td>
<td>Article 29.1.d. Attacks on computer systems</td>
<td>AUC largely compatible with BC</td>
</tr>
<tr>
<td>Article 5. System interference</td>
<td>Article 29.1.h. Attacks on computer systems</td>
<td>AUC largely compatible with BC</td>
</tr>
<tr>
<td>Article 6. Misuse of devices</td>
<td>Article 29.2.b. Computerized data breaches</td>
<td>AUC largely compatible with BC</td>
</tr>
<tr>
<td>Article 7. Computer-related forgery</td>
<td>Article 29.2.d. Computerized data breaches</td>
<td>AUC largely compatible with BC</td>
</tr>
<tr>
<td>Article 8. Computer-related fraud</td>
<td>Article 29.3. Content related offences</td>
<td>AUC largely compatible with BC</td>
</tr>
<tr>
<td>Article 9. Offences related to child pornography</td>
<td>Missing in AUC</td>
<td></td>
</tr>
<tr>
<td>Article 10. Offences related to infringement of copyright and related rights</td>
<td>Article 29.2.f. Computerized data breaches</td>
<td>AUC largely compatible with BC</td>
</tr>
<tr>
<td>Article 11. Attempt and aiding or abetting</td>
<td>Article 30.2. Criminal liability for legal persons</td>
<td>AUC largely compatible with BC</td>
</tr>
<tr>
<td>Article 12. Corporate liability</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Article 13. Sanctions and measures</td>
<td>Criminal sanctions</td>
<td></td>
</tr>
</tbody>
</table>
## Summary of Findings

<table>
<thead>
<tr>
<th>Article 13. Sanctions and measures</th>
<th>Criminal sanctions</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Article 3 Protocol. Dissemination of racist and xenophobic material through computer systems</td>
<td>Article 29.2.e. Content related offences</td>
<td>AUC largely compatible with Protocol to BC</td>
</tr>
<tr>
<td>Article 4 Protocol. Racist and xenophobic motivated threat</td>
<td>Article 29.2.f. Content related offences</td>
<td>AUC largely compatible with Protocol to BC</td>
</tr>
<tr>
<td>Article 5 Protocol. Racist and xenophobic motivated insult</td>
<td>Article 29.2.g. Content related offences</td>
<td>AUC largely compatible with Protocol to BC</td>
</tr>
<tr>
<td>Article 6 Protocol. Denial, gross minimisation, approval or justification of genocide or crimes against humanity</td>
<td>Article 29.2.h. Content related offences</td>
<td>AUC largely compatible with Protocol to BC</td>
</tr>
</tbody>
</table>

### Procedural law

<table>
<thead>
<tr>
<th>Article 14. Scope of procedural provisions</th>
<th></th>
<th>Missing in AUC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Article 15. Conditions and safeguards</td>
<td></td>
<td>Missing in AUC</td>
</tr>
<tr>
<td>Article 16. Expedited preservation of stored computer data</td>
<td>3.d. Procedural law</td>
<td>AUC largely compatible with BC</td>
</tr>
<tr>
<td>Article 17. Expedited preservation and partial disclosure of traffic data</td>
<td></td>
<td>Missing in AUC</td>
</tr>
<tr>
<td>Article 18. Production order</td>
<td></td>
<td>Missing in AUC</td>
</tr>
<tr>
<td>Article 19. Search and seizure of stored computer data</td>
<td>3.a and b. Procedural law</td>
<td>AUC incomplete but compatible with BC</td>
</tr>
<tr>
<td>Article 20. Real-time collection of traffic data</td>
<td></td>
<td>Missing in AUC</td>
</tr>
<tr>
<td>Article 21. Interception of content data</td>
<td>3.e. Procedural law</td>
<td>AUC compatible with BC but safeguards missing</td>
</tr>
</tbody>
</table>

### Jurisdiction

| Article 22. Jurisdiction |  | Missing in AUC |
## Summary of Findings

<table>
<thead>
<tr>
<th>International co-operation</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Article 23. General principles relating to international co-operation</td>
<td>Missing in AUC</td>
</tr>
<tr>
<td>Article 24. Extradition</td>
<td>Missing in AUC</td>
</tr>
<tr>
<td>Article 25. General principles relating to mutual assistance</td>
<td>Missing in AUC</td>
</tr>
<tr>
<td>Article 26. Spontaneous information</td>
<td>Missing in AUC</td>
</tr>
<tr>
<td>Article 27. Procedures pertaining to mutual assistance requests in the absence of applicable international agreements</td>
<td>Missing in AUC</td>
</tr>
<tr>
<td>Article 28. Confidentiality and limitation on use</td>
<td>Missing in AUC</td>
</tr>
<tr>
<td>Article 29. Expedited preservation of stored computer data</td>
<td>Missing in AUC</td>
</tr>
<tr>
<td>Article 30. Expedited disclosure of preserved traffic data</td>
<td>Missing in AUC</td>
</tr>
<tr>
<td>Article 31. Mutual assistance regarding accessing of stored computer data</td>
<td>Missing in AUC</td>
</tr>
<tr>
<td>Article 32. Trans-border access to stored computer data with consent or where publicly available</td>
<td>Implicit and broader in AUC</td>
</tr>
<tr>
<td>Article 33. Mutual assistance regarding the real-time collection of traffic data</td>
<td>Missing in AUC</td>
</tr>
<tr>
<td>Article 34. Mutual assistance regarding the interception of content data</td>
<td>Missing in AUC</td>
</tr>
<tr>
<td>Article 35. 24/7 Network</td>
<td>Missing in AUC</td>
</tr>
</tbody>
</table>
## Summary of Findings

<table>
<thead>
<tr>
<th>Electronic Transactions</th>
<th>Not specifically related to BC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Electronic Commerce</td>
<td></td>
</tr>
<tr>
<td>Contractual Obligations in Electronic Form</td>
<td></td>
</tr>
<tr>
<td>Security of Electronic Transactions</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Personal Data Protection</th>
<th>Not specifically related to BC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personal data protection</td>
<td></td>
</tr>
<tr>
<td>Institutional framework for the protection of personal data</td>
<td></td>
</tr>
<tr>
<td>Obligations relating to conditions governing personal data processing</td>
<td></td>
</tr>
<tr>
<td>The Data Subjects’ Rights</td>
<td></td>
</tr>
<tr>
<td>Obligations of the Personal Data Controller</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Promoting Cyber Security and Combatting Cybercrime</th>
<th>Not specifically related to BC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber Security Measures to be taken at National Level</td>
<td></td>
</tr>
</tbody>
</table>
### Definitions

- Xenophobic material
- Subscriber information
- Unauthorised Access
- Traffic Data
- Service Provider
- Computer Data
- Computer System

### Offences

- Sanctions and Measures
  - Corporate Liability
  - Aiding/Abetting
  - Copyright
  - Child Pornography
  - e-Fraud
  - e-Forgery
  - Misuse of Devices
  - System Interference
  - Data Interference
  - Illegal Interception
  - Illegal Access

- Jurisdiction
  - RT Collection Traffic
  - Interception
  - Search & Seizure
  - Production Order
  - Exp. Pres. of Traffic Data
  - Exp. Preservation of Data
  - Safeguards

### Procedural Powers

### International Cooperation

- 24/7 Network
- Interception
- Real-time Collection
- Accessing stored data
- Ex. Disc. of Traffic Data
- Trans-border Access
- Ex. Pres. of Stored Data
- Confederality
- Absence of agreements
- Spontaneous Information
- Mutual Assistance
- Extradition
- General Principles

### Consistency

- Consistent with international standard
- Not consistent but not conflicting
- Missing
<table>
<thead>
<tr>
<th>Definitions</th>
<th>Offences</th>
<th>Procedural Powers</th>
<th>International Cooperation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consistent with international standard</td>
<td>Not consistent but not conflicting</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Service Provider**

**Traffic Data**

**Unauthorised Access**

**Subscriber information**

**Computer Data**

**Computer System**

- Xenophobic material
- Copyright
- Aiding/Abetting
- Corporate Liability
- Child Pornography
- e-Fraud
- e-Forgery
- Misuse of Devices
- System Interference
- Data Interference
- Illegal Interception
- Illegal Access

**Sanctions and Measures**

- Jurisdiction
- Jurisdiction
- RT Collection Traffic
- Interception
- Search & Seizure
- Production Order
- Exp. Pres. of Traffic Data
- Exp. Preservation of Data
- Safeguards

**24/7 Network**

- Interception
- Real-time Collection
- Accessing stored data
- Ex. Disc. of Traffic Data
- Trans-border Access
- Ex. Pres. of Stored Data
- Confidentiality
- Absence of agreements
- Spontaneous Information
- Mutual Assistance
- Extradition
- General Principles

*Consistent with international standard*
Definitions

Consistent with international standard

Offences

Not consistent but not conflicting

Procedural Powers

International Cooperation

Missing
### Definitions
- Consistent with international standard
- Not consistent but not conflicting
- Missing

### Offences
- Xenophobic material
- Unauthorised Access
- Traffic Data
- Service Provider
- Computer Data
- Computer System

### Procedural Powers
- Jurisdiction
- RT Collection Traffic
- Interception
- Search & Seizure
- Production Order
- Exp. Pres. of Traffic Data
- Exp. Preservation of Data
- Safeguards

### International Cooperation
- 24/7 Network
- Interception
- Real-time Collection
- Accessing stored data
- Ex. Disc. of Traffic Data
- Ex. Pres. of Stored Data
- Confidentiality
- Absence of agreements
- Spontaneous Information
- Mutual Assistance
- Extradition
- General Principles
Comparative analysis: Malabo Convention of African Union and Budapest Convention on Cybercrime

**Imperative**

**Enabling Environment** to combat Cybercrime

Sovereign's/State’s *positive* obligation to *protect citizens* from (cyber)crime

**Impact**

*Missing* or *Inadequate* Legal Provisions *Prejudice* this *Objective*

Could *undermine existing* Best Practice *Legislation* and Processes in AU member states
Salient Examples of Issues
AUC: Unauthorised Access

- AUC Offence: “Gain or attempt to gain unauthorized access to part or all of a computer system or exceed authorized access”

- No definition of “unauthorized access”
AUC: Data Interference & System Interference

Data Interference

- Missing “without right”
  (i.e. missing unauthorised)

- Requirement of “fraudulently”
- (for data interference and illegal interception)
  – means offences legal if no element of fraud

- computer data
System interference

• NO “without right”
  (i.e. missing unauthorised)

• No mens rea (no without right or fraudulent – strict liability
  – Means that authorised system interference an offence

• Missing: damaging, deleting, or suppressing computer data
AUC: Misuse of Devices

- Does **not cover** production, sale, procurement for use, import, distribution of access codes and other computerized data

- Does **not cover** dual-use technologies (requires that device be “specially adapted” rather than “adapted primarily”)

- Does **not provide protection/carve out** for authorized testing or cybersecurity operations
AUC: e-Forgery, e-Fraud and racism/xenophobia-related offences

• Consistent with the Budapest Convention and the Additional Protocol

• One of the good examples of realization of Budapest Convention
• Largely consistent to the Budapest Convention

• Consistent in principle but lacks the necessary tests to determine authorized person acting on behalf of a legal person
AUC: Child Pornography

- Largely consistent with the Budapest Convention
- **Missing mens rea** element (intentionally/without right)
- Restricted definition of child pornography, **missing** the elements of:
  - **persons appearing to be minors** engaged in sexually explicit conduct;
  - **realistic images** representing minors engaged in sexually explicit conduct

*UN Protocol Rights of the Child on the sale of children, child prostitution and child pornography*
• Unclear scope of procedural provisions

• Missing **safeguards** against abuse of powers (especially in interception of content data)

• Missing the following procedural powers:
  • **Expedited** preservation and **partial disclosure** of traffic data (Article 17)
  • **Production** order (Article 18)
  • No provision for **seizure** of **electronic evidence** (A.19)
  • **Real-time** collection of **traffic data** (Article 20)
Provision corresponding to expedited preservation of data in AU is not an “expedited power” – requires warrant for judge and therefore may not be effective.

Provision corresponding to interception of content data is missing judicial safeguards and is open to abuse.
AUC: International Cooperation

• NO Binding/Suggested Legal Framework:

Article 28: International cooperation

1. Harmonization

State Parties shall ensure that the legislative measures and/or regulations adopted to fight against cyber-crime will strengthen the possibility of regional harmonization of these measures and respect the principle of double criminal liability.

2. Mutual legal assistance

State Parties that do not have agreements on mutual assistance in cyber-crime shall undertake to encourage the signing of agreements on mutual legal assistance in conformity with the principle of double criminal liability, while promoting the exchange of information as well as the efficient sharing of data between the organizations of State Parties on a bilateral and multilateral basis.

3. Exchange of information

State Parties shall encourage the establishment of institutions that exchange information on cyber threats and vulnerability assessment such as the Computer Emergency Response Team (CERT) or the Computer Security Incident Response Teams (CSIRTs).

4. Means of cooperation

State Parties shall make use of existing means for international cooperation with a view to responding to cyber threats, improving cyber security and stimulating dialogue between stakeholders. These means may be international, intergovernmental or regional, or based on private and public partnerships.
Double criminality (dual criminality) means a crime punished in both the country where a suspect is being held and the country asking for the suspect to be handed over or transferred to;

Limited only to:
- Extradition cases

BC: Mutual Assistance: applies to all cases (except Art 2-11 and Expedited Preservation)

[BC Article 25 – General principles relating to mutual assistance]
• Most **important** aspect of international or regional cybercrime instrument is: **functional legally binding framework** for criminal justice cooperation – Missing in AU Convention

• AU Convention provides **aspirational principles** - **no specific powers** that are necessary for effective international cooperation and combatting of cybercrimes

• **Infrastructure/Data Repository countries** - not **AU Convention members** – but are members of Budapest Convention
• Missing a functional international cooperation mechanism including the following provisions:

  – Article 23. General principles relating to international co-operation
  – Article 24. Extradition
  – Article 25. General principles relating to mutual assistance
  – Article 26. Spontaneous information
  – Article 27. Procedures pertaining to mutual assistance requests in the absence of applicable international agreements
  – Article 28. Confidentiality and limitation on use
  – Article 29. Expedited preservation of stored computer data
International Cooperation

• Missing a functional international cooperation mechanism including the following provisions:

  – Article 30. Expedited disclosure of preserved traffic data
  – Article 31. Mutual assistance regarding accessing of stored computer data
  – Article 32. Trans-border access to stored computer data with consent or where publicly available
  – Article 33. Mutual assistance regarding the real-time collection of traffic data
  – Article 34. Mutual assistance regarding the interception of content data
  – Article 35. 24/7 Network
Are BC and AUC complementary?

- AU Convention may offer limited value to AU member states due to:
  - no comprehensive procedural powers in relation to electronic evidence, and
  - no functional international cooperation mechanism

- **However, AU Convention and Budapest Convention are not in conflict with each other**
Are BC and AUC complementary?

• AU Convention may be interpreted as a set of **aspirational principles** that **still requires** a functional framework such as Budapest Convention to realize them.

• Draft language for Article 3 of the AU Convention mandated the use of the language provided for in the Budapest Convention:

  “**Member States shall take into account the approved language choice in international cybercrime legislation models such as the Council of Europe and the Commonwealth of Nations where necessary.**”
Are BC and AUC complementary?

• Certain language in the AU Convention appears to mandate Member States to leverage the Budapest Convention

  • “Considering that the goal of this Convention is to take on board internationally recognized best practices”

  • “State Parties shall make use of existing means for international cooperation”
Are BC and AUC complementary?

- Even though many provisions in the AU Convention are **missing** and others **inconsistent** with the Budapest Convention, the AU Convention is **not in conflict** with the Budapest Convention.

- **Problems** would arise if a state implemented vague provisions of the **AU Convention without support of the Budapest Convention**.
Towards a Collaborative Approach

- AU states could **build upon political commitment** of AU leaders in adopting the AU Convention through use of Budapest Convention to:
  - improve their **domestic cybercrime legislation** and
  - engage in international cooperation
<table>
<thead>
<tr>
<th>Definitions</th>
<th>Offences</th>
<th>Procedural Powers</th>
<th>International Cooperation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consistent with international standard</td>
<td>Not consistent but not conflicting</td>
<td></td>
<td>Missing</td>
</tr>
</tbody>
</table>

### AU Convention & Budapest Convention

#### Definitions
- Xenophobic material
- Subscriber information
- Unauthorised Access
- Traffic Data
- Service Provider
- Computer Data
- Computer System

#### Offences
- Corporate Liability
- Aiding/Abetting
- Copyright
- Child Pornography
- e-Fraud
- e-Forgery
- Misuse of Devices
- System Interference
- Data Interference
- Illegal Interception
- Illegal Access
- Illegal Access

#### Procedural Powers
- Jurisdiction
- RT Collection Traffic
- Interception
- Search & Seizure
- Production Order
- Exp. Pres. of Traffic Data
- Exp. Preservation of Data
- Safeguards

#### International Cooperation
- 24/7 Network
- Interception
- Real-time Collection
- Accessing stored data
- Ex. Disc. of Traffic Data
- Ex. Pres. of Stored Data
- Confidentiality
- Absence of agreements
- Spontaneous Information
- Mutual Assistance
- Extradition
- General Principles

### AU Convention & Budapest

#### AU Convention & Budapest

- AU Convention
- Budapest

#### Definitions

- Consistent with international standard
- Not consistent but not conflicting
- Missing
Questions

Thank you!

Zahid Jamil, Esq.
Barrister
zahid@jamilandjamil.com