GLACY+

Global Action on Cybercrime Extended

Action globale sur la cybercriminalité élargie

Version 20 November 2016

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

Based on a study by
Zahid Jamil (Pakistan)
for the GLACY+ Project

www.coe.int/cybercrime

Funded
by the European Union
and the Council of Europe

EUROPEAN UNION

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Implemented
by the Council of Europe

Contents

Contact
Cybercrime Programme Office of the
Council of Europe (C-PROC)
Tel +33-3-9021-4506
Email alexander.seger@coe.int

Disclaimer
This technical report does not necessarily reflect official positions of the Council of Europe or the European Union.

1 Introduction

The Budapest Convention on Cybercrime of the Council of Europe was opened for signature in November 2001. By August 2016, 49 States were Parties and a further 18 had signed it or been invited to accede. These included from the African continent Mauritius (Party), Ghana (invited), Morocco (invited), Senegal (invited) and South Africa (signed).[1]

In June 2014, in Malabo, member States of the African Union adopted the African Union Convention on Cyber Security and Personal Data Protection.[2]

By mid-2016, only 12 of the 54 African countries had basic substantive or procedural law provisions on cybercrime and electronic evidence in place.[3] Many others were in the process of drafting legislation with the African Union and Budapest Conventions serving as guidance.

The purpose of the present technical report is to analyse the compatibility or complementary of both treaties in order to facilitate support to African countries in the reform of their legislation on cybercrime and electronic evidence.[4]

The report is thus limited to the issue of cybercrime and electronic evidence and does not cover the sections of the African Union Convention dealing with "Electronic Transactions", "Personal Data Protection" or general matters related to "Cyber Security".

2 Scope of both treaties

The Budapest Convention is a criminal justice treaty with a specific focus on cybercrime and electronic evidence. It requires Parties (a) to criminalise a range of offences against and by means of computers, (b) to provide criminal justice authorities with procedural powers to secure electronic evidence in relation to any crime and (c) to engage in efficient international cooperation.

The first pillar on substantive criminal law covers in Articles 2 to 11, offences against (i) the confidentiality, integrity and availability of computer data and systems, (ii) computer-related offences, (iii) content-related offences and (iv) offences related to infringements of copyright and related rights. In the separate Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems ("Additional Protocol"), certain offences related to acts of a racist and xenophobic nature are dealt with.

The second pillar is a set of specific procedural provisions that describe in detail the powers that criminal justice authorities may exercise when investigating the criminal offences against and by means of computers established under the first pillar, but also when investigating any other offences where evidence may be found on computer systems. These powers must be subject to conditions and safeguards to protect the rights of individuals. In this respect, the Budapest Convention is not just a cybercrime convention but one that also provides the basis for collection of electronic evidence relating to other crimes, such as murder, terrorism, drug trafficking and other serious crime. Hence, it is effectively a convention on both cybercrime and electronic evidence.

The third pillar is an extension of the second pillar into the international arena, providing a mechanism for international cooperation in matters not only related to cybercrime but again to police to police and judicial cooperation in relation to any crime involving electronic evidence.

[1] http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

[2] https://ccdcoe.org/sites/default/files/documents/AU-270614-CSConvention.pdf

[3] See Appendix.

[4] This technical report is to facilitate capacity building and is not to be understood as an official position of the Council of Europe or of the European Union towards the African Union.

The Budapest Convention is backed up the Cybercrime Convention Committee, which among other things, assesses implementation of this treaty by the Parties, and by capacity building programmes.

The Budapest Convention thus, provides a comprehensive, operational and functional solution for the investigation and prosecution of cybercrime both domestically and between Parties, with a global reach.

The AU Convention is, on the one hand, broader than the Budapest Convention in that it covers:

- Chapter I – Electronic transactions
- Chapter II – Personal data protection
- Chapter III – Cyber security and cybercrime

Thus, the AU Convention is an attempt to unite different aspects related to information technology law and certain non-digital and non-criminal justice issues.

On the other hand, however, with regard to cybercrime and electronic evidence, the AU Convention criminalizes some but not all of the conduct foreseen under the Budapest Convention. Moreover, the AU Convention does not provide for the full set of procedural powers for investigating and prosecuting cybercrime and securing electronic evidence in domestic investigations. And finally, the AU Convention does not contain specific provisions and does not constitute a legal basis for international cooperation on cybercrime and electronic evidence.

Overall, however, it would seem that though provisions and aspects are missing, those provisions that are available within the AU Convention – in spite of inconsistencies – are largely not in conflict with the Budapest Convention.

3 AU Convention and Budapest Convention: differences and compatibility

The AU Convention represents a political commitment by African States to take measures on a range of issues, including cybercrime.

The AU Convention contains, in some form, the offences of the Budapest Convention. Several of the offences, in particular the provisions corresponding to electronic fraud and electronic forgery and content-related offences such as child pornography and offences related to xenophobia and racism are covered by the AU Convention and are largely consistent with the Budapest Convention. Moreover, certain high-level principles within the AU Convention appear to match various articles of the Budapest Convention.[5] In that sense, in principle, the Budapest Convention and the AU Convention appear to have a degree of compatibility.

At the same time, the AU Convention has limitations and is not fully consistent with the provisions of the Budapest Convention. For example:

- Almost all the offences under the AU Convention are missing appropriate *mens rea* elements, and therefore appear to criminalize legitimate conduct of law enforcement authorities and other conduct that should be lawful under international best practice.[6]

[5] Draft AU Convention in fact specifically mentioned the Budapest Convention in the following terms:
"Article III(1)(1) – Member States shall take into account the approved language choice in international cybercrime legislation models such as the language choice adopted by the Council of Europe and the Commonwealth of Nations where necessary."

[6] While the AU Covention delves into the area of exceeding authorization it opens the door to the issue but leaves it not only partially dealt with but narrows its application to the point where many offences would not fall within this definition and not viewed as cybercrime. The absence of the priniciple of "without right" being included in the

- Some provisions which have been included in the AU Convention but not in the Budapest Convention are somewhat unclear.[7]

- Some of the offences as noted in the provision-by-provision study below are not comprehensive and do not fully cover all ingredients and elements contained in the Budapest Convention.

- Most of the procedural powers provided for under the Budapest Convention are missing in the AU Convention. This includes "production orders" which are crucial to obtain data from service providers.

- The procedural powers which have been included in the AU Convention tend to be vaguely defined, to be incomplete and not to be subject to conditions and safeguards. This raises rule of law concerns. The vague nature of the procedural powers means that different African States are likely to implement these principles in a rather differen manner.

- Key definitions relating to procedural powers such as "service provider", "traffic data" and "subscriber information" are missing from the AU Convention. These concepts are essential for defining specific procedural powers to secure such data for criminal justice purposes.

- The most important aspect relating to an international or regional instrument on cybercrime is to create a functional framework for criminal justice cooperation between Parties. Whereas the Budapest Convention provides for an effective and fully-functional mechanism for international cooperation between State Parties, the AU Convention does not have such provisions altogether. Hence, on its own the AU Convention cannot assist its member states achieve their stated objective of harmonizing cybercrime domestic law and enabling cooperation against cybercrime between Parties.

While important provisions on cybercrime and electronic evidence are incomplete or missing in the AUC, overall, however, both treaties seem not to be in conflict with each other.

Budapest Convention on Cybercrime ("BC")	**African Union Convention on Cyber Security and Personal Data Protection ("AUC")**	**Comments**
Definitions		
Article 1.a "computer system"	Article 1. "computer system"	AUC different from BC
Article 1.b "computer data"	Article 1. "computerized data"	AUC incomplete but compatible with BC
Article 1.c "service provider"		Missing in AUC
Article 1.d "traffic data"		Missing in AUC
Protocol 189 Article 2 "racist and xenophobic material"	Article 1. "racist and xenophobic material"	AUC largely compatible with Protocol to BC
Article 18.3 "subscriber information"		Missing in AUC

offences means that some offences under the AU Convention are strict liability offences without any mens rea and may apply to conduct which is legal. Other offences under the AU Convention require "fraudulent" intent, that is, a much higher standard than that in the Budapest Convention, which means that conduct which is criminalized under the Budapest Convention (if done with intent and without right) would not constitute an offence under the AU Convention because under the AU Convention one must prove some form of deceit or deception. It may be that the problem here emanates from a mistranslation from French to English. In French "frauduleux" could mean dishonest but could also mean illegal and not necessarily "fraud" as undersood by the English civil or common law jurisprudence. Regardless, the issue merits redressal.

[7] For example, see Article 29(1)(d) of the AU Convention, which requires State Parties to take measures to make it an offence to remain or attempt to remain fraudulently in part or all of a computer system;

Budapest Convention on Cybercrime ("BC")	**African Union Convention on Cyber Security and Personal Data Protection ("AUC")**	**Comments**
Substantive criminal law		
Article 2. Illegal access	Article 29.1.a-c. Attacks on computer systems	AUC largely compatible with BC
Article 3. Illegal interception	Article 29.2.a. Computerized data breaches	AUC largely compatible with BC
Article 4. Data interference	Article 29.1. e-f. Attacks on computer systems	AUC largely compatible with BC
Article 5. System interference	Article 29.1.d. Attacks on computer systems	AUC largely compatible with BC
Article 6. Misuse of devices	Article 29.1.h. Attacks on computer systems	AUC largely compatible with BC
Article 7. Computer-related forgery	Article 29.2.b. Computerized data breaches	AUC largely compatible with BC
Article 8. Computer-related fraud	Article 29.2.d. Computerized data breaches	AUC largely compatible with BC
Article 9. Offences related to child pornography	Article 29.3. Content related offences	AUC largely compatible with BC
Article 10. Offences related to infringement of copyright and related rights		Missing in AUC
Article 11. Attempt and aiding or abetting	Article 29.2.f. Computerized data breaches	AUC largely compatible with BC
Article 12. Corporate liability	Article 30.2. Criminal liability for legal persons	AUC largely compatible with BC
Article 13. Sanctions and measures	Criminal sanctions	
Article 3 Protocol. Dissemination of racist and xenophobic material through computer systems	Article 29.2.e. Content related offences	AUC largely compatible with Protocol to BC
Article 4 Protocol. Racist and xenophobic motivated threat	Article 29.2.f. Content related offences	AUC largely compatible with Protocol to BC
Article 5 Protocol. Racist and xenophobic motivated insult	Article 29.2.g. Content related offences	AUC largely compatible with Protocol to BC
Article 6 Protocol. Denial, gross minimisation, approval or justification of genocide or crimes against humanity	Article 29.2.h. Content related offences	AUC largely compatible with Protocol to BC
Procedural law		
Article 14. Scope of procedural provisions		Missing in AUC
Article 15. Conditions and safeguards		Missing in AUC
Article 16. Expedited preservation of stored computer data	3.d. Procedural law	AUC largely compatible with BC
Article 17. Expedited preservation and partial disclosure of traffic data		Missing in AUC
Article 18. Production order		Missing in AUC
Article 19. Search and seizure of stored computer data	3.a and b. Procedural law	AUC incomplete but compatible with BC
Article 20. Real-time collection of traffic data		Missing in AUC
Article 21. Interception of content data	3.e. Procedural law	AUC compatible with BC but safeguards missing

Budapest Convention on Cybercrime ("BC")	**African Union Convention on Cyber Security and Personal Data Protection ("AUC")**	**Comments**
Jurisdiction		
Article 22. Jurisdiction		Missing in AUC
International co-operation		
Article 23. General principles relating to international co-operation		Missing in AUC
Article 24. Extradition		Missing in AUC
Article 25. General principles relating to mutual assistance		Missing in AUC
Article 26. Spontaneous information		Missing in AUC
Article 27. Procedures pertaining to mutual assistance requests in the absence of applicable international agreements		Missing in AUC
Article 28. Confidentiality and limitation on use		Missing in AUC
Article 29. Expedited preservation of stored computer data		Missing in AUC
Article 30. Expedited disclosure of preserved traffic data		Missing in AUC
Article 31. Mutual assistance regarding accessing of stored computer data		Missing in AUC
Article 32. Trans-border access to stored computer data with consent or where publicly available	3.a Procedural law	Implicit and broader in AUC
Article 33. Mutual assistance regarding the real-time collection of traffic data		Missing in AUC
Article 34. Mutual assistance regarding the interception of content data		Missing in AUC
Article 35. 24/7 Network		Missing in AUC
Electronic Transactions		Not specifically related to BC
	Electronic Commerce	
	Contractual Obligations in Electronic Form	
	Security of Electronic Transactions	
Personal Data Protection		Not specifically related to BC
	Personal data protection	
	Institutional framework for the protection of personal data	
	Obligations relating to conditions governing personal data processing	
	The Data Subjects' Rights	
	Obligations of the Personal Data Controller	
Promoting Cyber Security and Combatting Cybercrime		Not specifically related to BC
	Cyber Security Measures to be taken at National Level	

4 Conclusion: Towards complementarity of both treaties

Overall, the AU Convention as such would seem to be of limited value as a criminal justice instrument on cybercrime and electronic evidence, in particular given the shortcomings of the procedural law and the absence of provisions on international cooperation.

However, the AU Convention – with respect to cybercrime – may be interpreted as a set of aspirational principles that require a functional framework such as the Budapest Convention to realize them.

Many high-level principles in the AU Convention appear to mandate the adoption of internationally recognized best practices[8] and existing means of international cooperation[9]. The earlier draft of the AU Convention specifically mentioned the Budapest Convention.[10] In this light, one could build a case and argue that the intent of the drafters was to encourage countries to adopt operationally effective and functional treaties, such as the Budapest Convention.

The analysis carried out here suggests that, a priori, the provisions of the AUC regarding cybercrime are not in conflict with the Budapest Convention. However, problems may arise if a country were to implement limited or vague provisions of the AU Convention only. It would thus be advisable to follow the Budapest Convention from the outset when preparing domestic legislation. This would then also facilitate accession to the Budapest Convention without further amendments should a country wish to do so.

African States will need to cooperate with the authorities of countries in other regions of the world where electronic evidence is often stored or where service providers are located. The most relevant States in this respect are already Parties to the Budapest Convention. Joining this treaty would offer a legal framework for African countries to engage in cooperation with these countries.

In conclusion, the most sensible way ahead would be to underscore the complementarity of both treaties. This means building on the political commitment of African leaders to take on the challenge of cybercrime as expressed when adopting the African Union Convention, and supporting countries of Africa to make use of the Budapest Convention when improving domestic legislation, establishing domestic criminal justice capacities and engaging in international cooperation.

[8] Preamble of the AUC:
"Considering that the goal of this Convention is to …take on board **internationally recognized best practices**;"

[9] 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.

[10] Draft language of Article III(1)(1): Laws against cyber crime
Member States shall take into account the approved language choice in international cybercrime legislation models such as the language choice adopted by the **Council of Europe and the Commonwealth of Nations** where necessary.

5 Annex: Provisions of Budapest Convention against provisions of Malabo Convention

Comparison between the African Union Convention on Cyber Security and Personal Data Protection (AUC) and Convention on Cybercrime (BC)

African Union Convention on Cyber Security and Personal Data Protection ("AUC")		**Budapest Convention on Cybercrime ("BC")**	**Comments**
Definitions			
Article 1: Definitions			
AU	means the African Union;		
Child pornography	means any visual depiction, including any photograph, film, video, image, whether made or produced by electronic, mechanical, or other means**,** of sexually explicit conduct, where: a) the production of such visual depiction involves a minor; b) such visual depiction is a digital image, computer image, or computer generated image where a minor is engaging in sexually explicit conduct or when images of their sexual organs are produced or used for primarily sexual purposes and exploited with or without the child's knowledge; c) such visual depiction has been created, adapted, or modified to appear that a minor is engaging in sexually explicit conduct.	**Article 9 – Offences related to child pornography** 2 For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts: a a minor engaged in sexually explicit conduct; b a person appearing to be a minor engaged in sexually explicit conduct; c realistic images representing a minor engaged in sexually explicit conduct.	**AUC incomplete but largely compatible with BC** The inclusion of a definition and offence relating to child pornography is in line with international best practice. The inclusion of the word 'mechanical or other means' beyond electronic and digital means tends to extend the scope of the AUC beyond electronic and digital matters, and possibly may create some degree of inconsistency of the scope of the AUC and certain challenges related to implementation, though the intent behind it to cover as much of child pornography aspects is positive. The definition is also missing "b a person appearing to be a minor engaged in sexually explicit conduct;

African Union Convention on Cyber Security and Personal Data Protection ("AUC")		Budapest Convention on Cybercrime ("BC")	Comments
			c realistic images representing a minor engaged in sexually explicit conduct." Thus it is narrow and not as comprehensive as other definitions in international best practice. This would have the effect of not criminalizing several forms of child pornography and provide safe harbor and protection to criminals whose content would fall within the scope of the missing definitions. Therefore, it would not constitute an offence under the AUC if a person appearing to be minor but who is technically over the age of eighteen is depicted for the gratification of the child pornography viewer. Further, it would also not constitute an offence under the AUC to visually depict realistic images of children in the form of pornographic cartoons (e.g. hentai). Many AU member states already have comprehensive child pornography offences within their existing legislation. Rather than improving upon these legislations, State Parties would in fact be mandated by the AUC to regress and create loopholes in their legislations. Regardless of the inconsistencies identified, this does not by itself represent a conflict between the two instruments. However, in order to achieve greater efficiency and to enable AU states to be able to cooperate globally to combat cybercrime, using the

African Union Convention on Cyber Security and Personal Data Protection (“AUC”)		**Budapest Convention on Cybercrime (“BC”)**	**Comments**
			provisions of the BC to complement and add as a patch to the existing AUC may be useful as members of the BC tend to be those whom members of the AUC seek cooperation in combatting cybercrime with. As a result, the patch offered by the BC and its complementarity with the AUC offers a solution. Such an approach may remedy any shortcomings in the AUC whilst enabling cooperation between AUC member states and members of the BC.
Computer system	means an electronic, magnetic, optical, electrochemical, or other high speed data processing device or a group of interconnected or related devices performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device or devices;	**Article 1 – Definitions** For the purposes of this Convention: a "computer system" means any device or a group of interconnected or related devices**, one or more of which, pursuant to a program, performs automatic processing of data;**	**AUC different from BC** The physics of a computer system has been defined, as opposed to its functional elements which are essential with respect to the constituents and elements of cybercrime offences. The exclusion of program or data processing should be remediated within the AUC. The functional elements that constitute a computer system may be dealt with by adopting relevant language from the BC. This is an example of how the BC can complement and create consistency if adopted by AU member states.
Computerized data	means any representation of facts, information or concepts in a form suitable for processing in a computer system;	b "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;	**AUC incomplete but compatible with BC** Computerized data ordinarily means data that has been converted from non-digital to digital data, and the use of the term in this context in the AUC may create confusion. This may particularly impact Commonwealth countries with common law traditions,

African Union Convention on Cyber Security and Personal Data Protection ("AUC")		**Budapest Convention on Cybercrime ("BC")**	**Comments**
			where the use of grammar and language and its interpretation can have an impact on the definition in question. This definition appears not to include the functional aspects necessary for properly defining certain forms of cybercrime, i.e. the inclusion of the term "program". It is important to include within the definition of computer data the fact that data includes programs, since it distinguishes between other forms of data which do not include programs. Although certain functional aspects are missing from this definition, the BC and the AUC are not inconsistent in this regard. However, by adding language from the BC to this definition, the definition shall become comprehensive.
Critical Cyber/ICT Infrastructure	means the cyber infrastructure that is essential to vital services for public safety, economic stability, national security, international stability and for the sustainability and restoration of critical cyberspace;	**Not defined in BC.** **Examples :** **42 U.S. Code § 5195c - Critical infrastructures protection** (e)Critical infrastructure defined In this section, the term "critical infrastructure" means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on	The definition of Critical Cyber/ICT Infrastructure is defined in terms of the vital nature of the infrastructure itself, rather than the effect of its damage, destruction or incapacitation. This definition adopted by the AUC may be considered relatively more subjective and open to interpretation, which may pose problems in clearly identifying critical infrastructure. This term is not defined in the Budapest Convention. However, an amendment[11] to the UK Computer Misuse Act in 2015

[11] S. 3ZA was inserted on 03.05.2015 by Serious Crime Act 2015 (c. 9), ss. 41(2), 88(1); S.I. 2015/820, reg. 2(a)

African Union Convention on Cyber Security and Personal Data Protection ("AUC")		**Budapest Convention on Cybercrime ("BC")**	**Comments**
		security, national economic security, national public health or safety, or any combination of those matters. **UK Computer Misuse Act Section 3ZA** Unauthorised acts causing, or creating risk of, serious damage (2) Damage is of a "material kind" for the purposes of this section if it is— (a) damage to human welfare in any place; (b) damage to the environment of any place; (c) damage to the economy of any country; or (d) damage to the national security of any country. (3) For the purposes of subsection (2)(a) an act causes damage to human welfare only if it causes— (a) loss to human life; (b) human illness or injury; (c) disruption of a supply of money, food, water, energy or fuel; (d) disruption of a system of communication; (e) disruption of facilities for transport; or (f) disruption of services relating to health.	represents a recent instance of international best practice legislation pertaining to critical infrastructure.
Damage	any impairment to the integrity or availability of data, a program, a system, or information;	Not defined in BC.	This definition is only used in the offence relating to data interference under Article 29(1)(e) and (f), whereas the term "damage" ought to be included in other forms of damage (i.e. damage to computer systems). The inclusion of the word "system" creates

African Union Convention on Cyber Security and Personal Data Protection ("AUC")		Budapest Convention on Cybercrime ("BC")	Comments
			confusion since the term "damage" is not used in the offence related to system interference under Article 29(d) of the AUC. If it is intended to deal with systems and not just data, the definition of damage is incomplete as the element of hindering with the functioning of a system without right appears to be absent. Either the word "system" should be removed and the term being defined changed to "data damage", or the element of hindering with the functioning of a computer system should be inserted into this definition. The element of availability is a useful addition to the AUC. However, the definition of damage is missing the element of suppression of data, which has also not been adequately covered by Article 29(1)(e) and (f). The term suppression is a broader term and therefore while availability of data is rightly mentioned, it is useful to also cover the concept of suppression.
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;	Article 25 – General principles relating to mutual assistance (5) Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the	**AUC too narrow.** The way dual criminality is defined (i.e. restricted to the concept of extradition) it is inconsistent with international law. The principle of dual criminality also has a broader application that applies to international cooperation and exchange of data. This definition is particularly problematic because it applies to a principle which has an overriding and overarching effect in the AUC that worst prohibits and at

African Union Convention on Cyber Security and Personal Data Protection ("AUC")		Budapest Convention on Cybercrime ("BC")	Comments
		requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.	best limits certain act of cross border cooperation from being be taken in the case of dual criminality. This has two effects. First, it over-applies the principle of dual criminality in cases where it would not ordinarily be applicable, thus, limiting instances of international best practice cross border cooperation against cybercrime. Second, it under-applies the principle of dual criminality by limiting it only to the cases related to extradition. Therefore, it incorrectly applies in both cases where dual criminality should be invoked and where dual criminality should not be in issue. The concept of dual criminality within the AUC applies as an overarching principle to negate any international activity in case of dual criminality as defined here. As a result, it is inconsistent with and conflicts with various provisions of BC where cooperation to share information is required or exists regardless of the principle of dual criminality. In limited cases, particularly where the international cooperation for exercise of power that is being sought is not particularly intrusive, such as Article 29 Section 3 of BC. Under this provision of the BC, dual criminality is not a precondition for expedited preservation of stored computer data. Hence, international cooperation for preservation of stored computer data is mandated regardless of whether the offence related to which the requesting country is making the request is also an offence in the

African Union Convention on Cyber Security and Personal Data Protection (“AUC”)		Budapest Convention on Cybercrime (“BC”)	Comments
			requested country. However, the overall impact of the incorrect definition of dual criminality appears to be narrow and limited. Since by its very definition it limits its applicability to only those cases where extradition is sought. It thus, narrows itself to such a degree that it becomes irrelevant in cases where no extradition is sought. Hence, as defined in the AUC, it neither enables nor restricts international cooperation for collection and exchange of data. Therefore, were the BC to be used as a patch for the AUC, this aspect of the AUC would not conflict with the BC.
Exceeds authorized access	means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter;	**Explanatory Report to Budapest Convention** 38. A specificity of the offences included is the express requirement that the conduct involved is done "without right". It reflects the insight that the conduct described is not always punishable per se, but may be legal or justified not only in cases where classical legal defences are applicable, like consent, self defence or necessity, but where other principles or interests lead to the exclusion of criminal liability. The expression "without right" derives its meaning from the context in which it is used. Thus, without restricting how Parties may implement the concept in their domestic law, it may refer to conduct undertaken without authority (whether legislative, executive, administrative,	**AUC incomplete. While not incompatible with BC this creates problems for offences related to “attacks on computer systems”.** It is a challenge to use term “exceeds authorization” without defining the terms “unauthorized” or “authorized”. (This is particularly when these terms are used to establish offenses under the Convention.)[12] The AUC does not define the term “authorized access” or “unauthorized access”, which would be foundational and a precursor to the concept of exceeding authorized access. Exceeding authorized access is a subset and a form of unauthorized access. Therefore, it is restricting both this definition and the AUC

[12] The BC does not define authorization or the term it uses as “without right” within the Convention but at the same time does not define subsets of the term without defining the larger set. Moreover, the BC does provide an elaboration of the term within its Explanatory document.

African Union Convention on Cyber Security and Personal Data Protection (“AUC”)		**Budapest Convention on Cybercrime (“BC”)**	**Comments**
		judicial, contractual or consensual) or conduct that is otherwise not covered by established legal defences, excuses, justifications or relevant principles under domestic law. The Convention, therefore, leaves unaffected conduct undertaken pursuant to lawful government authority (for example, where the Party’s government acts to maintain public order, protect national security or investigate criminal offences). Furthermore, legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices should not be criminalised. Specific examples of such exceptions from criminalisation are provided in relation to specific offences in the corresponding text of the Explanatory Memorandum below. It is left to the Parties to determine how such exemptions are implemented within their domestic legal systems (under criminal law or otherwise). **Example** **UK Computer Misuse Act** **Section 17 – Interpretation** (5) Access of any kind by any person to any program or data held in a computer is unauthorised if— (a) he is not himself entitled to control access of the kind in question to the program or data; and (b) he does not have consent to access by	to only define exceeding unauthorized access as this means the larger set of unauthorized access is not criminalized and creates a gaping loophole within the AUC in this respect. Therefore, the larger set or superset of instances of access generally are not covered in in parts of the AUC. Also, significantly, though the term unauthorized access has been used in the AUC, it remains undefined anywhere. The BC elaborates upon the equivalent of the term “without right” in its Explanatory document. Unauthorized access, and the concept of unauthorized, is foundational and basic to any cybercrime instrument. Without being able to properly define authorization, any cybercrime instrument would lack the necessary ingredients to properly criminalize cybercrime conduct. Not defining these terms and using them within the offences leads to vagueness and ambiguity in its use and application. Consequently, it has a disharmonizing effect as a result of and inconsistent/conflicting application in each case within a particular country, and between different African countries because it becomes a question of interpretation rather than a standard. This runs counter to the purpose of the AUC which is to harmonize cybercrime legislation across the African Union. (see A.___of the AUC) Moreover, the definition only covers obtaining/altering information (i.e. certain

African Union Convention on Cyber Security and Personal Data Protection (“AUC”)		**Budapest Convention on Cybercrime (“BC”)**	**Comments**
		him of the kind in question to the program or data from any person who is so entitled	kinds of interference), and that also when the initial access to the system is with authorization. To the extent that there is no concept of “without right” (unauthorized) as compared to the BC (elaborated within its Expanatory document), this is inconsistent with the BC. However, this may be remediated by adoption of the principle of “without right” (unauthorized) from the BC, as done in the UK CMA, which represents an instance of international best practice language.
Information	means **any element of knowledge** likely to be represented with the aid of **devices** and to be used, conserved, processed or communicated. Information may be expressed in **written, visual, audio, digital and other forms**;		By departing from the normal and widely understood grammatical definition of information, there is a natural distinction created between the specific meaning of the term under the AUC versus information generally, allowing lawyers to argue what may or may not fall within the term as defined by the AUC. Hence, this definition unnecessarily creates a narrow definition and allows room for argument on behalf of defence attorneys, creating an obstruction in the investigation/prosecution of offences without any benefit. Also, this definition would appear redundant given the definition of data. In fact, the inclusion of a definition of information creates ambiguity and uncertainty. It is unclear what constitutes an element of knowledge or how one would distinguish between knowledge likely to be represented

African Union Convention on Cyber Security and Personal Data Protection ("AUC")		**Budapest Convention on Cybercrime ("BC")**	**Comments**
			by devices and used etc. as opposed to instances where this is not the case. It is also unclear what is meant by other forms, this seems to be a catch all included as a safety net. Hence, though on the one hand the definition is not carefully drafted to cover all types of information by narrowing it to elements of knowledge, on the other hand it is drafted to be broad and catch all in terms of the medium that may be associated with the term. As can be seen this is both unnecessarily convoluted and falls short of being constructive.
Child or Minor	means every human being below the age of eighteen (18) years in terms of the African Charter on the Rights and Welfare of the Child and the United Nations Convention on the Rights of the Child respectively;	**Article 9 – Offences related to child pornography** 3 For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.	**AUC compatible with BC.** This definition is consistent with BC.
Racism and xenophobia in information and telecommunication technologies	means any written material, **picture** or any other representation of ideas or theories which advocates or encourages or incites hatred, discrimination or violence against any person or group of persons for reasons based on race, colour, ancestry**,** national or ethnic origin or religion;	**Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems** Article 2 – Definition 1 For the purposes of this Protocol: "racist and xenophobic material" means any written material, any **image** or any other representation of ideas or theories, which advocates, promotes or incites hatred, discrimination or violence,	**AUC largely compatible with Protocol to BC.** This definition is largely consistent with BC. However, it is missing the condition regarding advocating or encouraging or inciting hatred, discrimination or violence against any person or group of persons for reasons based upon religion "if used as a pretext for any of these factors" (namely race, colour, descent or national or ethnic origin). The Additional Protocol to BC

African Union Convention on Cyber Security and Personal Data Protection ("AUC")		**Budapest Convention on Cybercrime ("BC")**	**Comments**
		against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion **if used as a pretext for any of these factors**. **Explanatory Report to the Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems** 21. The notion of "religion" often occurs in international instruments and national legislation. The term refers to conviction and beliefs. The inclusion of this term as such in the definition would carry the risk of going beyond the ambit of this Protocol. However, religion may be used as a pretext, an alibi or a substitute for other factors, enumerated in the definition. "Religion" should therefore be interpreted in this restricted sense.	envisages the interpretation of the term "religion" in this restricted sense, as there are times when religion may be used as a cover or an excuse to protect what is in substance and essence racism or xenophobia. In particular, this would legalize much of the terrorist content produced by groups such as Boko Haram, Daesh and ISIS and would undermine the usefulness of this for African Union Member States. The use of the term "picture" rather than "image" as in the Additional Protocol to BC limits the scope of this definition. The term "picture" it may be argued may exclude paintings, computer-generated images which are often used to as mediums mediums to commit the offences relating to racist and xenophobic information in the AUC. This may be a result of translation of the AUC from French to English but requires remediation through explanatory notes or other means so that its application in Anglophone African Union states is consistent and includes all forms of images. Therefore, the shortcoming of the above elements, though may create an inconsistency, may not rise to the level of a conflict between the two instruments. This shortcoming may also easily be addressed by AU member states adopting and then implementing the BC, thereby using both the instruments to complement each other.

African Union Convention on Cyber Security and Personal Data Protection (“AUC”)		**Budapest Convention on Cybercrime (“BC”)**	**Comments**
Service provider	***Absent/Missing***	c "service provider" means: i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and ii any other entity that processes or stores computer data on behalf of such communication service or users of such service.	**Missing in AUC.** The AUC is missing the definition of a service provider although the term is used in the procedural sections. This is essential for the several procedural powers mandated by BC, namely Article 17 – Expedited preservation and partial disclosure of traffic data, Article 18 – Production order, Article 20 – Real-time collection of traffic data, Article 21 – Interception of content data and international cooperation under Article 30 – Expedited disclosure of preserved traffic data. This may be read into the AUC if the BC is adopted as a patch to bridge the gaps of the AUC, as the definition of service provider has not only been mandated under the BC but also adopted by international best practice legislation.
Traffic data	***Absent/Missing***	d "traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication’s origin, destination, route, time, date, size, duration, or type of underlying service.	**Missing in AUC.** The AUC is missing the definition of traffic data which is critical to procedural powers under Article 16 –Expedited preservation of stored computer data Article 17 – Expedited preservation and partial disclosure of traffic data Article 20 –Real-time collection of traffic data and international cooperation under Article 30 – Expedited disclosure of preserved traffic data and Article 33 –Mutual assistance in the real-time collection of traffic data.

African Union Convention on Cyber Security and Personal Data Protection (“AUC”)		**Budapest Convention on Cybercrime (“BC”)**	**Comments**
			The absence of a definition of “traffic data” distinguishable from “content data” may pose problems in clearly defining procedural powers, and may result in either granting narrower a or more likely broader powers in a warrant meant to be restricted for instance to traffic data or subscriber information, thus, excluding necessary safeguards available in the BC in this respect and posing civil liberties, due process and human rights concerns. The absence of a definition of traffic data can be remediated by AU member states by adopting the BC and implementing the given definition in their domestic legislations. This is another good example of where the BC may be used as a patch to fill the gaps where the AUC might be found to be deficient or missing provisions necessary for the combat of cybercrime.
Subscriber information	***Absent/Missing***	3 For the purpose of this article, the term “subscriber information” means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established: a the type of communication service used, the technical provisions taken thereto and the period of service; b the subscriber’s identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the	**Missing in AUC.** The AUC is missing the definition of subscriber information which is essential to the procedural power under Article 18 – Production order. Subscriber information as defined in BCBC refers to information relating to subscribers of services held by service providers. As observed in the Explanatory Report to BC, as “subscriber information includes forms of data other than computer data, a special provision has been included… to address this

African Union Convention on Cyber Security and Personal Data Protection ("AUC")		Budapest Convention on Cybercrime ("BC")	Comments
		service agreement or arrangement; c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.	type of information"[13] Hence, the absence of a separate definition of subscriber information in the AUC may effect the particular procedural powers in relation to service providers and obligations that ought to be placed upon service providers in relation to such information as under international best practice. For procedural powers that have appropriate safeguards consistent with civil liberty and due process principles it is necessary that the distinction between various categories of data/information are specified. In particular this is necessary for making or giving effect to cross border requests for cooperation. It is thus, vital that the AUC clearly distinguish between the different forms of data as the procedural powers necessary for an effective framework to combat cybercrime may vary depending on the type of data it pertains to. Further, in order to be consistent with international cooperation framework already in place, it is important to distinguish between content data, traffic data, subscriber information and computer data so that requested states may be able to understand and process requests for a specific type of data or information. However, if the BC is viewed as a complementary patch to the AUC, the

[13] Paragraph 177 of the Explanatory Report to BC.

African Union Convention on Cyber Security and Personal Data Protection (“AUC”)		**Budapest Convention on Cybercrime (“BC”)**	**Comments**
			concept of subscriber information as well as the separate procedural powers in relation to the same may be read as complementing and bridging this gap within the AUC.
CHAPTER III – PROMOTING CYBER SECURITY AND COMBATING CYBERCRIME			
Section I: Cyber Security Measures to be taken at National Level			
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 c**hoice of language that is used in international best practices.**		**AUC compatible with BC.** This provision shares an overarching principle with BC and gives State Parties authorization to prosecute cyber offences. As this provision mandates State Parties to consider “choice of language that is used in international best practices”, the AUC may be interpreted to mandate State Parties to use BC, which lays down principles for international best practice.
	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**	*Title 3 – 24/7 Network* **Article 35 – 24/7 Network** 1 Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to	**AUC compatible with BC.** This provision could be used as an enabling provision to achieve consistency with the provisions of BC. This provision contains general language which may achieve such consistency and provide legal mandate to much needed international cooperation

African Union Convention on Cyber Security and Personal Data Protection (“AUC”)		**Budapest Convention on Cybercrime (“BC”)**	**Comments**
	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.	computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures: a the provision of technical advice; b the preservation of data pursuant to Articles 29 and 30; c the collection of evidence, the provision of legal information, and locating of suspects. 2 a A Party’s point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis. b If the point of contact designated by a Party is not part of that Party’s authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis. 3 Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.	frameworks for AUC states if interpreted to mandate the establishment of investigation agencies for investigating cybercrime and especially 24-7 networks for international cooperation.
	3. Rights of citizens In adopting legal measures in the area of cyber security and establishing the framework for implementation thereof, 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	**Article 15 – Conditions and safeguards** 1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section 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	**Missing in AUC.** The AUC generally stipulates that measures taken should respect rights. While this is helpful it does not extend to providing necessary principles for establishing safeguards necessary given the intrusive nature of investigative powers to combat cybercrime. Application of existing rights

African Union Convention on Cyber Security and Personal Data Protection (“AUC”)		**Budapest Convention on Cybercrime (“BC”)**	**Comments**
	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.	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. 2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia*, include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure. 3 To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.	will not necessarily achieve these objectives since the new rights extended for law enforcement require new and updated forms of safeguards, conditions, limits and protections to be introduced which do not currently exist under the law of most countries, particularly in most AUC states' legislation. Conversely, Article 15 BC stipulates a number of specific safeguards and conditions to be put in place to limit procedural powers.
	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 as elements of critical information infrastructure; and, in this regard, proposing more severe sanctions for criminal activities on ICT systems in these sectors, as well as	**T-CY Guidance Note #6 on Critical Information Infrastructure Attacks** A Party may foresee in its domestic law a sanction that is unsuitably lenient for critical information infrastructure attacks, and it may not permit the consideration of aggravated circumstances or of attempt, aiding or abetting. This may mean that Parties need to consider amendments to their domestic law. Parties should ensure, pursuant to Article 13, that criminal offences	**AUC largely compatible with BC.** The AUC mandating State Parties to impose more severe penalties on offences involving critical information infrastructure is consistent with the Budapest Convention.

African Union Convention on Cyber Security and Personal Data Protection (“AUC”)		**Budapest Convention on Cybercrime (“BC”)**	**Comments**
	measures to improve vigilance, security and management.	related to such attacks “are punishable by effective, proportionate and dissuasive sanctions, which include the deprivation of liberty”. For legal persons this may include criminal or non-criminal sanctions, including monetary sanctions. Parties may also consider aggravating circumstances, for example, if critical information infrastructure attacks affect a significant number of systems or cause considerable damage, including deaths or physical injuries.	
International Cooperation			
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.		**AUC incomplete.** The principle of harmonization is broad however there are two shortcomings. First, the definition of dual criminality in the AUC is narrow and inconsistent with BC. [14] Second, this provision refers to respecting dual criminality across the board, while under BC in certain circumstances for instance preservation of data, the absence of dual criminality is not an excuse (i.e. Article 29 of BC). It also does not provide any substance or nuisance as to what aspects or matters that need to be criminalized. It therefore remains aspirational rather than a substantive or

[14] See comments on definition of the term “Dual Criminality”

African Union Convention on Cyber Security and Personal Data Protection ("AUC")		**Budapest Convention on Cybercrime ("BC")**	**Comments**
			functional providing necessary practical mechanisms in this regard. Further, this provision speaks about "legislative measures and/or regulations". This is very narrow and does not address conventions/treaties. Mutual legal assistance treaties or bilateral arrangements. Moreover, the term "regional harmonization" appears to exclude harmonization of international cooperation mechanisms and harmonization of procedures, all of which are necessary for an effective cybercrime regime. Although the high-level principles in this provision may not be entirely consistent with the BC broadly, they call for the harmonization of legislative measures between member states, which is one of the key objectives of the BC. In this respect, both instruments complement each other and aim to achieve the same objective. It would be useful that the slightly more detailed principles and their elaboration in this regard available in the BC is adopted and implemented by AUC member states as a tool to implement this high-level principle mandated by the AUC.
	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**	**25 – General principles relating to mutual assistance** 1 The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences	**AUC incomplete and narrower than BC.** The MLA provisions are the cornerstone and one of the most important substantive elements of a cybercrime instrument. Unfortunately, it appears that there is a

African Union Convention on Cyber Security and Personal Data Protection ("AUC")		Budapest Convention on Cybercrime ("BC")	Comments
	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.	related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. 2 Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35. 3 Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or email, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication. 4 Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence. 5 Where, in accordance with the provisions of this chapter, the requested Party is	complete lack of substance in this regard in the AUC making it deficient in most important and core element of such an instrument. Effectively the heart of a treaty on cybercrime is absent from this treaty. At most it mentions only a couple of the numerous international law principles and mechanisms for cooperation required by any international best practice instrument to make it useful and functional for the purposes of use by states. As mentioned above, the principle of double criminality in this and other provisions of the AUC through their limited definition and expansive application appears to be contradictory and contrary to International law [see comment on Article 25]. Further, as mentioned above, the AUC is deficient when dealing with the core aspects of international cooperation. Not only are principles in general missing, but powers and specific provisions relating to the international cooperation are altogether absent. While the AUC deals with certain aspects in very high-level and hyperbole, it does not provide a framework or a mechanism for State Parties to actually cooperate with one another. In fact, the principles are so high-level without any functional elements that they appear to be more aspirational as opposed to functional in order to operate at any level for internationally cooperation in matters

African Union Convention on Cyber Security and Personal Data Protection ("AUC")		Budapest Convention on Cybercrime ("BC")	Comments
		permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.	related to cybercrime. This undermines the usefulness and efficacy of the AUC as a relevant instrument with respect to international cooperation or even regional cooperation with respect to cybercrime. As an instance of the, specific international cooperation provisions which are conspicuous by their absence Article 28 addresses international cooperation at a very high level generally declaring that there should be harmonization, without any further substance as to what elements an in which way are they to harmonize. This achieves the opposite as it may leave it open to each member state to implement their one version and any aspect they consider relevant in this context, instead thereby causing disharmony. Hence, the AUC does not provide the necessary ingredients that are required by any international convention for cooperation on cybercrime and does not provide detailed language as provided under BC. Due to its paucity of explanatory or detailed language, it falls short of even a high level comment on measures for international cooperation. It may be possible to leverage this paucity interpreting the broad nature, and statements for adoption of international instruments and next practice to be

African Union Convention on Cyber Security and Personal Data Protection ("AUC")		Budapest Convention on Cybercrime ("BC")	Comments
			interpreted as encouraging the adoption of the various aspects within BC be they the procedural provisions or international cooperation (particularly if Article 28(1) of the AUC is read with Article 25(1) of the AUC, which speaks about international best practice). This would allow remediation by the BC of the missing elements of international cooperation mechanisms. However, because both refer to "language" and "legislation" and therefore restrict themselves to legislative matters with respect to national law and do not provide a cross-border international binding framework which is the basic benefit one derives from an international convention, it fails to provide the third pillar (international cooperation) required under any international convention to combat cybercrime. The efficacy of an international convention on cybercrime is that default mutual legal assistance provisions should have been included in the AUC that could have been applied in the absence of a bilateral treaty. It therefore appears that the AUC misses its own objective as set out in this sub-article. However, since the AUC does encourage parties to work on a "multilateral basis", this may be interpreted as an encouragement to states within the AU to become parties to multilateral conventions to fight cybercrime

African Union Convention on Cyber Security and Personal Data Protection ("AUC")		**Budapest Convention on Cybercrime ("BC")**	**Comments**
			i.e. only one being BC. With such an interpretation the AUC would not be in conflict with the BC but rather could complement the BC and encourages parties to join the BC.
	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).		This is about CERT to CERT cooperation and not relevant for criminal justice.
	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.		**Possibly an encouragement to make use of the BC.** In terms of international cooperation this is probably the most valuable provision of the AUC. Though Article 28(2) of the AUC implies the following, this provision specifically, without any reservation or exception provides that State Parties are not merely encouraged but "shall make use of **existing means for international cooperation**…" and thus appears to mandate State Parties to use instruments such as the BC. It further clarifies this by the use of the language "international, intergovernmental or regional" the first two of which include the BC. Reading Article 28(2) and (4), together with Article 25(1) "existing means for

African Union Convention on Cyber Security and Personal Data Protection (“AUC”)		Budapest Convention on Cybercrime (“BC”)	Comments
			international cooperation” implies use of BC since it is the only existing international instrument providing a mechanism for international cooperation in regards to combatting cybercrime. This interpretation is further supported by the fact that the original language in the draft version of the AUC in relation to this provision specifically named the BC.[15] This, therefore, appears to mandate the use of the BC as a complement to the AUC to fill those areas relating to international cooperation that have not been dealt with in sufficient detail by the AUC. Were one to argue the opposite and by interpretation exclude the possibility of reading in the BC, and apply the inconsistencies strictly it would lead to at least two significant problems for the member states of the AUC. (a) It creates an obstacle for AUC member states to both receive and seek international cooperation with respect to cybercrime and the cross-border exchange of electronic evidence. (b) It creates an obstacle for AUC member states to adopt and accede

[15] Draft AU Convention in fact specifically mentioned the Budapest Convention in the following terms:
“Article III(1)(1) – Member States shall take into account the approved language choice in international cybercrime legislation models such as the language choice adopted by the Council of Europe and the Commonwealth of Nations where necessary.“

African Union Convention on Cyber Security and Personal Data Protection ("AUC")		Budapest Convention on Cybercrime ("BC")	Comments
			to the BC and in this respect also receive and seek international cooperation with respect to cybercrime and the cross-border exchange of electronic evidence from member states of the BC, particularly those states from whom African states generally tend to seek data and exchange information. As a result, such a strict interpretation would do a disservice to the interests of the AUC state parties. The only interpretation that serves the interests of the AUC member states is to view both instruments as complementary.
	Absent/Missing	**Chapter III – International co-operation** **Section 1 – General principles** *Title 1 – General principles relating to international co-operation* **Article 23 – General principles relating to international co-operation** The Parties shall co-operate with each other, in accordance with the provisions of this chapter, and through the application of relevant international instruments on international cooperation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or	**Missing in AUC.** The AUC is missing provisions akin to: • Article 23 – General principles relating to international co-operation, • Article 24 – Extradition, • Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements, • Article 28 – Confidentiality and limitation on use and specific provisions including • Article 29 –Expedited preservation of stored computer data, • Article 30 – Expedited disclosure of preserved traffic data ,

African Union Convention on Cyber Security and Personal Data Protection ("AUC")		Budapest Convention on Cybercrime ("BC")	Comments
		for the collection of evidence in electronic form of a criminal offence.	• Article 31 –Mutual assistance regarding accessing of stored computer data, • Article 33 – Mutual assistance in the real-time collection of traffic data, and • Article 34 –Mutual assistance regarding the interception of content data. Thus specific international cooperation provisions are almost entirely missing. This impedes mutual assistance and international cooperation with respect to the investigation and prosecution of cybercrimes. However, the high-level principles contained in Article 28 of the AUC appear to not only complement but also mandate the BC. AUC state parties adopting and implementing the BC alongside the AUC therefore provides a complete and functional international cooperation framework.
	Absent/Missing	**Article 24 – Extradition** 1 a This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty. b Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for	**Missing in AUC.** Extradition in relation to cybercrime is not covered by the AUC. This may hinder prosecution of cybercriminals committing offences in a State Party while not within the territory of that State Party.

African Union Convention on Cyber Security and Personal Data Protection ("AUC")		Budapest Convention on Cybercrime ("BC")	Comments
		under such arrangement or treaty shall apply. 2 The criminal offences described in paragraph 1 of this article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them. 3 If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article. 4 Parties that do not make extradition conditional on the existence of a treaty shall recognize the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves. 5 Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition. 6 If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of	

African Union Convention on Cyber Security and Personal Data Protection ("AUC")		Budapest Convention on Cybercrime ("BC")	Comments
		the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as for any other offence of a comparable nature under the law of that Party. 7 a Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and address of each authority responsible for making or receiving requests for extradition or provisional arrest in the absence of a treaty. b The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.	
	Absent/Missing	**Article 26 – Spontaneous information** 1. A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a	**Missing in AUC.** Article 26 is an important provision as it offers a legal basis for law enforcement to inform another Party pro-actively and for the receiving Party to act upon such information. The absence of this enabling provision means that law enforcement in possession of evidence that they believe may be useful

African Union Convention on Cyber Security and Personal Data Protection ("AUC")		**Budapest Convention on Cybercrime ("BC")**	**Comments**
		request for co-operation by that Party under this chapter. 2. Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.	to the authorities of another state for investigating or prosecuting cybercrime do not have a legal (hence, evidentially admissible) basis on which to proactively share the evidence with the other state. They have to wait for an official request from the other state. This creates a causality dilemma (chicken and egg situation) where the law presumes that a state would ask for something it does not know about from another state. The absence of this enabling provision will prove to be a substantial shortcoming for any AUC member state that wishes to proactively pass on evidence related to cybercrime thereby negatively impacting cybercrime cooperation within the AUC.
	Absent/Missing	**Article 27 – Procedures pertaining to mutual assistance requests in the absence of** **applicable international agreements** 1 Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof. 2 a Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual	**Missing in AUC.** The absence of any detailed provision explaining procedures pertaining to mutual assistance requests in the absence of applicable international agreements may hinder effective international cooperation between State Parties. This gap can be bridged through the adoption of provisions of the BC by AU member states as the adoption of these additional principles would not be inconsistent with the AUC.

African Union Convention on Cyber Security and Personal Data Protection (“AUC”)		Budapest Convention on Cybercrime (“BC”)	Comments
		assistance, the execution of such requests or their transmission to the authorities competent for their execution. b The central authorities shall communicate directly with each other; c Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph; d The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times. 3 Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party. 4 The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or b it considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests. 5 The requested Party may postpone action	

African Union Convention on Cyber Security and Personal Data Protection ("AUC")		Budapest Convention on Cybercrime ("BC")	Comments
		on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities. 6 Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary. 7 The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be given for any refusal or postponement of the request. The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly. 8 The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed. 9 a In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases, a copy shall be sent at the same time to the central authority of the	

African Union Convention on Cyber Security and Personal Data Protection (“AUC”)		**Budapest Convention on Cybercrime (“BC”)**	**Comments**
		requested Party through the central authority of the requesting Party. b Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol). c Where a request is made pursuant to sub-paragraph a. of this article and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so. d Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party. e Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority.	
	Absent/Missing	**Article 28 – Confidentiality and limitation on use** 1 When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and the requested Parties, the provisions of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or	**Missing in AUC.** There is no specific provision on confidentiality or limitation of use of data shared between State Parties through international cooperation. Absence of this provision that protects state interests and creates trust between both the requesting and requested state thereby enabling

African Union Convention on Cyber Security and Personal Data Protection ("AUC")		Budapest Convention on Cybercrime ("BC")	Comments
		legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof. 2 The requested Party may make the supply of information or material in response to a request dependent on the condition that it is: a kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or b not used for investigations or proceedings other than those stated in the request. 3 If the requesting Party cannot comply with a condition referred to in paragraph 2, it shall promptly inform the other Party, which shall then determine whether the information should nevertheless be provided. When the requesting Party accepts the condition, it shall be bound by it. 4 Any Party that supplies information or material subject to a condition referred to in paragraph 2 may require the other Party to explain, in relation to that condition, the use made of such information or material.	cooperation would mean that there may be a substantially lesser degree of cooperation between AU member states. Member states would have to apply conditions when cooperating without a legal basis providing certainty that their conditions would be enforceable. However, if Article 28(4) of the AUC is read to mandate the incorporation of the provisions of BC, it can be inferred that State Parties are mandated to implement the principles of Article 28 in their domestic legislations.
	Absent/Missing	**Section 2 – Specific provisions** *Title 1 – Mutual assistance regarding provisional measures* **Article 29 – Expedited preservation of stored computer data** 1 A Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, located within the territory of that other Party and in respect of	**Missing in AUC.** There is no corresponding provision in the AUC. This may impede international cooperation. This is probably the most important and most used cross border provision when combatting cybercrime and crimes where

African Union Convention on Cyber Security and Personal Data Protection ("AUC")		Budapest Convention on Cybercrime ("BC")	Comments
		which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data. 2 A request for preservation made under paragraph 1 shall specify: a the authority seeking the preservation; b the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts; c the stored computer data to be preserved and its relationship to the offence; d any available information identifying the custodian of the stored computer data or the location of the computer system; e the necessity of the preservation; and f that the Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data. 3 Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation. 4 A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored data may, in respect of offences other than those established in accordance with Articles 2 through 11 of this	electronic evidence is involved. Being one of the most important international cooperation provisions in the BC, its absence in the AUC proves to be of a substantial shortcoming. However, this may be overcome by AUC member states adopting the BC and therefore filling and bridging this gap.

African Union Convention on Cyber Security and Personal Data Protection (“AUC”)		**Budapest Convention on Cybercrime (“BC”)**	**Comments**
		Convention, reserve the right to refuse the request for preservation under this article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled. 5 In addition, a request for preservation may only be refused if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests. 6 Where the requested Party believes that preservation will not ensure the future availability of the data or will threaten the confidentiality of or otherwise prejudice the requesting Party’s investigation, it shall promptly so inform the requesting Party, which shall then determine whether the request should nevertheless be executed. 7 Any preservation effected in response to the request referred to in paragraph 1 shall be for a period not less than sixty days, in order to enable the requesting Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such a request, the data shall continue to be preserved pending a decision on that request.	
	Absent/Missing	**Article 30 – Expedited disclosure of preserved traffic data**	**Missing in AUC.**

African Union Convention on Cyber Security and Personal Data Protection (“AUC”)		**Budapest Convention on Cybercrime (“BC”)**	**Comments**
		1 Where, in the course of the execution of a request made pursuant to Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted. 2 Disclosure of traffic data under paragraph 1 may only be withheld if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.	There is no corresponding provision in the AUC. This may impede international cooperation. This shortcoming does not constitute a conflict between the AUC and the BC. However, in order to ensure effective international cooperation, the provisions of the BC may be used as a patch to the existing provisions of the AUC.
	Absent/Missing	**Article 31 – Mutual assistance regarding accessing of stored computer data** 1 A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29. 2 The requested Party shall respond to the request through the application of international instruments, arrangements	**Missing in AUC.** There is no corresponding provision in the AUC. This may impede international cooperation. This gap may be bridged through the adoption of provisions of the BC by AU member states as the adoption of these additional principles would not be inconsistent with the AUC.

African Union Convention on Cyber Security and Personal Data Protection (“AUC”)		**Budapest Convention on Cybercrime (“BC”)**	**Comments**
		and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter. 3 The request shall be responded to on an expedited basis where: a there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or b the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.	
	3. Procedural law a) State Parties shall take the necessary legislative measures to ensure that where the data stored in a computer system or in medium where computerized data can be stored in the territory of a State Party, are useful in establishing the truth, the court applied to may carry out a search to access all or part of a computer system through another computer system, where the said data are accessible from or available to the initial system;	**Article 32 – Trans-border access to stored computer data with consent or where publicly available** A Party may, without the authorisation of another Party: a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.	**Implicit and broader in AUC.** Article 32b BC allows for access to a computer systems in another Party to the BC under very limited conditions. Voluntary consent is required. The procedural law (section 3a) AUC allows for searches of a connect computer system also without consent. The BC has a search and seizure provision where such searches to connected systems are limited to systems “in its territory” (Article 19.2 BC).
	Absent/Missing	**Article 33 – Mutual assistance regarding the real-time collection of traffic data** 1 The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory	**Missing in AUC.** There is no corresponding provision in the AUC. This may impede international cooperation. This gap can be easily bridged through the adoption of provisions of the BC by AU member states as the adoption of

African Union Convention on Cyber Security and Personal Data Protection (“AUC”)		**Budapest Convention on Cybercrime (“BC”)**	**Comments**
		transmitted by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law. 2 Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.	these additional principles would not be inconsistent with the AUC.
	Absent/Missing	**Article 34 – Mutual assistance regarding the interception of content data** The Parties shall provide mutual assistance to each other in the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws.	**Missing in AUC.** There is no corresponding provision in the AUC. This may impede international cooperation. This gap can be easily bridged through the adoption of provisions of the BC by AU member states as the adoption of these additional principles would not be inconsistent with the AUC.
	Absent/Missing	**Article 35 – 24/7 Network** 1 Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures: a the provision of technical advice; b the preservation of data pursuant to	**Missing in AUC.** There is no specific provision in the AUC regarding the establishment of a 24/7 point-of-contact for the purposes of international cooperation. This gap can be easily bridged through the adoption of provisions of the BC by AU member states as the adoption of these additional principles would not be inconsistent with the AUC.

African Union Convention on Cyber Security and Personal Data Protection ("AUC")		**Budapest Convention on Cybercrime ("BC")**	**Comments**
		Articles 29 and 30; c the collection of evidence, the provision of legal information, and locating of suspects. 2 a A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis. b If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis. 3 Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.	
Section II: Criminal Provisions			
Substantive Criminal Law			
Article 29: Offences specific to Information and Communication Technologies	**1. Attacks on computer systems** State Parties shall take the necessary legislative and/or regulatory measures to make it a criminal offence to: a) Gain or attempt to gain unauthorized access to part or all of a computer system or exceed authorized access;	**Article 2 – Illegal access** Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a	Although this provision appears to be consistent with BC, when read with the definitions which relate to this offence, it becomes apparent that this provision is inconsistent as the element of 'without right' (unauthorized) is missing. This would mean that under the AUC illegal access would be a strict liability offence. The use of the language "unauthorized access" while consistent with international

African Union Convention on Cyber Security and Personal Data Protection ("AUC")		Budapest Convention on Cybercrime ("BC")	Comments
		computer system that is connected to another computer system.	best practice is meaningless in the absence of a definition of what constitutes unauthorized conduct. The existing definition of exceeding unauthorized access is both technically incorrect and ambiguous.[16] The definition of the term unauthorized is critical because every conduct done on an information system is "primarily or largely" done in the absence of authorization – therefore it is a foundational definition, be it for access or for any other activity in relation to a computer system. This provision also deals with exceeding authorization. The AUC thus, defines exceeding authoirsation (subset of general unauthorised conduct) without defining unauthorised in general. In essence defining an exception to the rule without defining the rule. Thus, on the one hand it narrows its application to the point where many offences may not fall within this definition and may not be viewed as cybercrime. Whilst on the other the absence of "without right" means that some offences under the AUC are strict liability offences without any mens rea and may apply to conduct which is legal. A complementary approach with the adoption of both instruments will ensure

[16] See comments on definition of the term "exceeds authorized access"

African Union Convention on Cyber Security and Personal Data Protection ("AUC")		Budapest Convention on Cybercrime ("BC")	Comments
			that the state of cybercrime and substantive offences within AUC member states is brought up to meet the minimum threshold required for criminalization of conduct termed as cybercrime internationally.
	b) Gain or attempt to gain unauthorized access to part or all of a computer system or exceed authorized access with intent to commit another offence or facilitate the commission of such an offence;		The provision is consistent with BC and international best practice.
	c) Remain or attempt to remain fraudulently in part or all of a computer system;		This is one of the most technically incorrect and legally unsound provisions in the AU and there is no such offence present in BC or any international best practice instrument. In particular, the inclusion of fraudulent intent creates complications because it only criminalizes "remaining" for the purpose of causing economic loss or gain or with an attempt to misrepresent or dishonesty, whereas Article 29(1)(a) and (b) do not require this. The conduct described in this provision is merely a continuation of (a) and (b) – one wouldn't expect the mens rea to be different and of a higher threshold. It is also unclear what constitutes "Remain" – i.e. for what period one would have to be present in part or all of a computer system. The conduct of remaining is not recognized as an offence in most countries, particularly those from whom cooperation is sought and therefore states which adopt this language

African Union Convention on Cyber Security and Personal Data Protection ("AUC")		**Budapest Convention on Cybercrime ("BC")**	**Comments**
			run into the problem of an absence of dual criminality. The creation of an offence which will not fulfil the criteria of dual criminality would by definition prevent any international cooperation, which would be prohibited by the AUC itself. Although this provision is also inconsistent with the BC, it is not in conflict with any particular provision of the BC. However, its use or implementation does cause the insertion of an absurdity in international law.
	d) Hinder, distort or attempt to hinder or distort the functioning of a computer system;	**Article 5 – System interference** Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed **intentionally**, the serious hindering without right of the functioning of a computer system by **inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data**.	- AUC is missing element of without right - No means of system interference specified in the AUC (e.g. inputting, transmitting, damaging computer data). - Requirement that the hindering be serious is missing in the AUC This provision attempts to address system interference however the absence of specified conduct that constitutes hindering creates ambiguity and uncertainty, and may fail to encompass conduct intended to be criminalized. Further, there is no mens rea element for this offence under the AUC and therefore this provision fails to cover authorized acts of intelligence and law enforcement agencies. This also means that hindering or distorting of the functioning of a computer

African Union Convention on Cyber Security and Personal Data Protection ("AUC")		**Budapest Convention on Cybercrime ("BC")**	**Comments**
			system without any malicious intent and regardless of whether it was authorized is strictly a criminal offence under the AUC – this would mean any authorised distortion by a user of their own data –which is legal conduct - would constitute a criminal offence. The ingredient that the hindering of the computer system be serious is missing, which may criminalize, particularly in the absence of any mens rea element, brief and inadvertent hindrances caused to internet services. The elements of inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data are missing, which are all essential components of system interference. The absence of certain key elements in related to this offence in the AUC may be remedied if AU member states adopt corresponding language from the BC as a patch to this provision.
	e) Enter or attempt to enter data fraudulently in a computer system; f) Damage or attempt to damage, delete or **attempt to delete**, deteriorate or attempt to deteriorate, alter or **attempt to alter**, **change or attempt to change** computer data fraudulently.	**Article 4 – Data interference** 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed **intentionally**, the damaging, deletion, deterioration, alteration or **suppression of computer data without right.** 2 A Party may reserve the right to require	- AUC is missing element of without right - inappropriate use of aggravated mens rea element of fraudulently in the AUC - the AUC is missing the element of suppression of computer data These provisions attempt to address data

African Union Convention on Cyber Security and Personal Data Protection ("AUC")		Budapest Convention on Cybercrime ("BC")	Comments
		that the conduct described in paragraph 1 result in serious harm.	interference however they fail to do so since they are missing the element of suppression of computer data. The use of the term "fraudulently" is inconsistent (in fact in conflict with) the standard of the BC A.4(1) "…when committed **intentionally**, the damaging, deletion, deterioration, alteration or suppression of computer data **without right**" which does not require fraud to be proved. This basically means that conduct which constitutes an offence of data interference under the BC's A. 4(1) would not be criminalized under the AUC's A.29(1)(f). The reference to "computer data" in clause (f) creates uncertainty as this term has not been defined in the AUC. The absence of certain key elements in related to this offence in the AUC may be remedied if AU member states adopt corresponding language from the BC as a patch to this provision.
	h) Take the necessary legislative and/or regulatory measures to make it a criminal offence to unlawfully produce, sell, import, possess, disseminate, offer, cede or make available computer equipment, program, or any device or data designed or **specially** adapted to commit offences, or unlawfully generate or produce a password, an access code or similar computerized data allowing	**Article 6 – Misuse of devices** 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right: a the production, sale, **procurement for use**, import, distribution or otherwise making available of:	- AUC is missing element of without right - AUC does not cater to dual use technologies as term 'specially adapted' is used in AUC rather than 'adapted primarily' as in the BC - production, sale, procurement for use, import, distribution of access codes and

African Union Convention on Cyber Security and Personal Data Protection ("AUC")		Budapest Convention on Cybercrime ("BC")	Comments
	access to part or all of a computer system.	i a device, including a computer program, designed or adapted **primarily for the purpose of committing any of the offences established in accordance with Articles 2 through 5;** ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches. 2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system. 3 Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making	other computerized data not covered by the AUC - AUC does not provide immunity to activities such as authorized testing or protection of computer systems The term "specially adapted" as against "primarily adapted" in BCBC raises the threshold of what is and what is not a virus. Dual-use technology primarily used to perpetrate an offence may not specially have been designed or adapted to commit an offence because it is not its primary objective. It becomes its sole objective. While one may argue that the section provides more safeguards by not criminalizing the production/use of dual use technologies, it makes it much more difficult to prosecute cases as it is very difficult to prove that it is specially designed for that one purpose. Only the conduct "generate or produce" have been used in relation to passwords, access codes or similar computerized data. Conduct such as the production, sale, procurement for use, import, distribution may not be covered by the limited scope of this The AUC lacks adequate safeguards to protect authorized testing and protection of computer system as in sub-article 2 of

African Union Convention on Cyber Security and Personal Data Protection (“AUC”)		**Budapest Convention on Cybercrime (“BC”)**	**Comments**
		available of the items referred to in paragraph 1 a.ii of this article.	Article 6 of BC. Innovation in Africa may be deemed to be criminal conduct as a result of this omission.
	2. Computerized Data Breaches State Parties shall take the necessary legislative and/or regulatory measures to make it a criminal offence to: a) Intercept or attempt to intercept computerized data fraudulently by technical means during non-public transmission to, from or within a computer system;	**Article 3 – Illegal interception** Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when **committed intentionally**, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, **including electromagnetic emissions from a computer system carrying such computer data.** A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system. **Explanatory Report to BC on Cybercrime** 57. The creation of an offence in relation to "electromagnetic emissions" will ensure a more comprehensive scope. Electromagnetic emissions may be emitted by a computer during its operation. Such emissions are not considered as ‘data’ according to the definition provided in Article 1. However, data can be reconstructed from such emissions. Therefore, the interception of data from electromagnetic emissions from a computer system is included as an offence under this provision.	This article, which is titled “computerized data breaches” does not deal with the offence of data confidentiality breaches, including an adequate framework to effectively deal with third parties who monetize or politicize such breaches of data (e.g. Wiki Leaks, Panama Papers. Edward Snowden) or aid or abet or facilitate breaches of data. This would mean that breaching confidentiality of African states is not appropriately covered under this article. This provision is missing the element of ‘including electromagnetic emissions from a computer system carrying such computer data’. As observed in Paragraph 7 of the Explanatory Report to BC on Cybercrime, such emissions although not considered data, may be intercepted and used to create data. The absence of this language in the AUC may render interception of electromagnetic emissions such as Wi-Fi communication legal. The absence of any mens rea requirement suggests even the actions of investigation agencies may fall under the scope of this section, which may render conducting investigations impossible.

African Union Convention on Cyber Security and Personal Data Protection ("AUC")		**Budapest Convention on Cybercrime ("BC")**	**Comments**
	b) Intentionally input, alter, delete, or suppress computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless of whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches;	**Article 7 – Computer-related forgery** Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.	This provision is consistent with Article 7 of BC and probably represents one of the best incorporations of this provision into an international document. However, the reference to "computer data" creates uncertainty as this term has not been defined in the AUC.
	c) Knowingly use data obtained fraudulently from a computer system;		This provision is inconsistent with BC and international best practice. Typically (with some exceptions) the use of leaked data once it has been publicly disseminated or becomes available does not constitute an offence. The provision deals with a complex area by means of a sweeping criminalising provision which is inadequate.
	d) Fraudulently procure, for oneself or for another person, **any benefit** by inputting, altering, deleting or suppressing computerized data or **any other form of interference** with the functioning of a computer system;	**Article 8 – Computer-related fraud** Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by: a any input, alteration, deletion or suppression of computer data, b any interference with the functioning of a computer system, with fraudulent **or dishonest intent** of procuring, without right, an **economic benefit** for oneself or	This provision is well-conceived. Although one could argue that the element of fraudulently does provide a certain degree of protection, the absence of the actus reus of committing this conduct without authorization is missing and may create uncertainty. While interference is defined under BC, the language "any form of interference" in the absence of a definition under the AUC is open to interpretation and may fail to cover

African Union Convention on Cyber Security and Personal Data Protection ("AUC")		**Budapest Convention on Cybercrime ("BC")**	**Comments**
		for another person.	the conduct intended to be addressed under this provision. The reference to "computer data" creates uncertainty as this term has not been defined in the AUC.
	e) Even through negligence, process or have personal data processed without complying with the preliminary formalities for the processing;		This provision is beyond the scope of this cybercrime review since it deals with data protection issues.
	f) Participate in an association formed or in an agreement established with a view to preparing or committing one or several of the offences provided for under this Convention.	**Article 11 – Attempt and aiding or abetting** 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed. 2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c of this Convention. 3 Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.	The criminalization of aiding and abetting offences is consistent with BC and international best practice. Attempting certain conduct, particularly that conduct defined in Article 28 (Offences specific to Information and Communication Technologies) has been criminalized under the AUC.
	3. Content related offences **1.** State Parties shall take the necessary	**Article 9 – Offences related to child pornography** 1 Each Party shall adopt such legislative and	To the extent that the AUC addresses child pornography in a manner that is largely consistent with BC, this is a positive step.

African Union Convention on Cyber Security and Personal Data Protection (“AUC”)		Budapest Convention on Cybercrime (“BC”)	Comments
	legislative and/or regulatory measures to make it a criminal offence to: a) Produce, **register,** offer, **manufacture,** make available, disseminate and transmit **an image or a representation of** child pornography through a computer system; b) Procure for oneself or for another person, **import or have imported, and export or have exported** an image or representation of child pornography through a computer system; c) Possess an image or representation of child pornography in a computer system or on a computer data storage medium; d) Facilitate or provide access to images, documents, sound or representation of a pornographic nature to a minor;	other measures as may be necessary to establish as criminal offences under its domestic law, when **committed intentionally and without right,** the following conduct: a producing child pornography for the purpose of its distribution through a computer system; b offering or making available child pornography through a computer system; c distributing or transmitting child pornography through a computer system; d procuring child pornography through a computer system for oneself or for another person; e possessing child pornography in a computer system or on a computer-data storage medium.	However, all the offences related to child pornography in this sub-article are missing the element of mens rea. It is unclear what is meant by register and manufacture – this language appears redundant given the use of other more suitable language. Although the definition of child pornography does not have the aspect of “image or representation”, it is useful that it is included in this offence. The terms import and export are not appropriate in the context of data.
	e) **Create, download, disseminate** or make available in any form **writings, messages, photographs, drawings or any other presentation of ideas or theories** of racist or xenophobic nature through a computer system;	**Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems** **Article 3 – Dissemination of racist and xenophobic material through computer systems** 1 Each Party shall adopt such legislative and other measures as may be necessary to	The AUC includes creation of and downloading racist and xenophobic material through a computer system rather than merely disseminating or making such material available. This exceeds the scope of the Additional Protocol to BC and may be over-criminalizing. The absence of any mens rea with this offence is also inconsistent with the Additional Protocol to BC.

African Union Convention on Cyber Security and Personal Data Protection (“AUC”)		**Budapest Convention on Cybercrime (“BC”)**	**Comments**
		establish as criminal offences under its domestic law, when committed **intentionally and without right**, the following conduct: distributing, or otherwise making available, racist and xenophobic material to the public through a computer system. 2 A Party may reserve the right not to attach criminal liability to conduct as defined by paragraph 1 of this article, where the material, as defined in Article 2, paragraph 1, advocates, promotes or incites discrimination that is not associated with hatred or violence, provided that other effective remedies are available. 3 Notwithstanding paragraph 2 of this article, a Party may reserve the right not to apply paragraph 1 to those cases of discrimination for which, due to established principles in its national legal system concerning freedom of expression, it cannot provide for effective remedies as referred to in the said paragraph 2.	Given the definition of Racism and xenophobia in information and telecommunication technologies, this language is redundant and creates uncertainty.
	f) Threaten, through a computer system, to commit a criminal offence against a person for the reason that they belong to a group distinguished by race, colour, descent, national or ethnic origin or religion where such membership serves as a pretext for any of these factors, or against a group of persons which is distinguished by any of	**Article 4 – Racist and xenophobic motivated threat** 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed **intentionally and without right**, the following conduct: threatening, through a computer system, with the commission of a serious criminal offence as defined under its	The absence of any mens rea with this offence is inconsistent with the Additional Protocol of BC.

African Union Convention on Cyber Security and Personal Data Protection (“AUC”)		**Budapest Convention on Cybercrime (“BC”)**	**Comments**
	these characteristics;	domestic law, (i) persons for the reason that they belong to a group, distinguished by race, colour, descent or national or ethnic origin, as well as religion, if used as a pretext for any of these factors, or (ii) a group of persons which is distinguished by any of these characteristics. 2 A Party may either: a require that the offence referred to in paragraph 1 of this article has the effect that the person or group of persons referred to in paragraph 1 is exposed to hatred, contempt or ridicule; or b reserve the right not to apply, in whole or in part, paragraph 1 of this article.	
	g) Insult, through a computer system, persons for the reason that they belong to a group distinguished by race, colour, descent, national or ethnic origin, or religion **or political opinion**, if used as a pretext for any of these factors, or against a group of persons distinguished by any of these characteristics;	**Article 5 – Racist and xenophobic motivated insult** 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: insulting **publicly**, through a computer system, (i) persons for the reason that they belong to a group distinguished by race, colour, descent or national or ethnic origin, as well as religion, if used as a pretext for any of these factors; or (ii) a group of persons which is distinguished by any of these characteristics. 2 A Party may either:	This provision although largely consistent with the Additional Protocol of BC, mandates an offence to insult, through a computer system, persons for the reason that they belong to a group distinguished by political opinion. This not only exceeds the scope of the offence as in the Additional Protocol of BC, but also appears to be in contravention of Article 25(3) of the AUC, which talks about rights of citizens. The absence of any mens rea with this offence is also inconsistent with the Additional Protocol of BC. This provision extends to private communications, which goes beyond the scope of BC and also appears to be

African Union Convention on Cyber Security and Personal Data Protection ("AUC")		**Budapest Convention on Cybercrime ("BC")**	**Comments**
		a require that the offence referred to in paragraph 1 of this article has the effect that the person or group of persons referred to in paragraph 1 is exposed to hatred, contempt or ridicule; or b reserve the right not to apply, in whole or in part, paragraph 1 of this article.	inconsistent with Article 25(3) of the AUC.
	h) Deliberately deny, approve or justify acts constituting genocide or crimes against humanity through a computer system.	**Article 6 – Denial, gross minimisation, approval or justification of genocide or crimes against humanity** 1 Each Party shall adopt such legislative measures as may be necessary to establish the following conduct as criminal offences under its domestic law, when committed **intentionally and without right**: distributing or otherwise making available, through a computer system to the public, material which denies, **grossly minimises**, approves or justifies acts constituting genocide or crimes against humanity, **as defined by international law and recognised as such by final and binding decisions of the International Military Tribunal, established by the London Agreement of 8 August 1945, or of any other international court established by relevant international instruments and whose jurisdiction is recognised by that Party.** 2 A Party may either a require that the denial or the gross minimisation referred to in paragraph 1 of this article is committed with the intent to incite hatred, discrimination or violence against any	Although this provision tries to take from the Additional Protocol to BC, it lacks the necessary element of gross minimization, which is an integral constituent of the corresponding provision in the Additional Protocol to BC.

African Union Convention on Cyber Security and Personal Data Protection (“AUC”)		Budapest Convention on Cybercrime (“BC”)	Comments
		individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors, or otherwise b reserve the right not to apply, in whole or in part, paragraph 1 of this article.	
	2. State Parties shall take the necessary legislative and/or regulatory measures to make the offences provided for under this Convention criminal offences. When such offences are committed under the aegis of a criminal organization, they will be punishable by the maximum penalty prescribed for the offense.		This provision attempts to address corporate liability but it has limited application since it only deals with severity of offences.
	3. State Parties shall take the necessary legislative and/or regulatory measures to ensure that, in case of conviction, national courts will give a ruling for confiscation of the materials, equipment, instruments, computer program, and all other devices or data belonging to the convicted person and used to commit any of the offences mentioned in this Convention.		Confiscation deals with convicted persons and articles used to commit the offence, but may not include proceeds of crime and thus has limited application.
	4. Offences relating to electronic message security measures State Parties shall take the necessary legislative and/or regulatory measures to ensure that digital evidence in criminal cases is admissible to establish offenses under national criminal law, provided such evidence has been presented during proceedings and discussed before the judge, that the person from whom it originates can be duly identified, and that it has been made out and retained in a manner capable		This provision mandates State Parties to ensure the admissibility of digital evidence in criminal cases and is consistent with international best practice.

African Union Convention on Cyber Security and Personal Data Protection ("AUC")		**Budapest Convention on Cybercrime ("BC")**	**Comments**
	of assuring its integrity.		
Article 30: Adapting certain offences to Information and Communication Technologies	**1. Property Offences** a) State Parties shall take the necessary legislative and/or regulatory measures to criminalize the violation of property such as theft, fraud, handling of stolen property, abuse of trust, extortion of funds and blackmail involving computer data; b) State Parties shall take the necessary legislative and/or regulatory measures to consider as aggravating circumstances the use of information and communication technologies to commit offences such as theft, fraud, handling of stolen property, abuse of trust, extortion of funds, terrorism and money laundering; c) State Parties shall take the necessary legislative and/or regulatory measures to specifically include "by means of digital electronic communication" such as the Internet in listing the means of public dissemination provided for under the criminal law of State Parties; d) State Parties shall take the necessary criminal legislative measures to restrict access to protected systems which have been classified as critical national defence infrastructure due to the critical national security data they contain.		Property offences may address fraud but the language is not completely consistent with BC. Nonetheless, the language is not inconsistent with BC and does serves a positive and useful purpose in terms of investigating and prosecuting crime. However, it may be noted that the reference to "computer data" in paragraph (a) creates uncertainty as this term has not been defined in the AUC.
	2. Criminal liability for legal persons State Parties shall take the necessary legislative measures to ensure that legal persons other than the State, local	**Article 12 – Corporate liability** 1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in	**AUC more narrow but largely compatible with BC.** This provision is missing the tests by which it is determined that natural

African Union Convention on Cyber Security and Personal Data Protection ("AUC")		**Budapest Convention on Cybercrime ("BC")**	**Comments**
	communities and public institutions can be held responsible for the offences provided for by this Convention, committed on their behalf by their organs or representatives. The liability of legal persons does not exclude that of the natural persons who are the perpetrators of or accomplices in the same offences.	accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on: a a power of representation of the legal person; b an authority to take decisions on behalf of the legal person; c an authority to exercise control within the legal person. 2 In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority. 3 Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative. 4 Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.	persons/organs/ representatives were acting on behalf of the legal persons and thus, it will be difficult to determine whether individuals were acting in their own capacity or on behalf of the legal person. This may have both an overcriminalising and an under criminalising effect depending upon the interpretation and application of a court. At the very least it may lead to inconsistent and diverging application contrary to the AUC's objective of harmonisation. The AUC furthermore requires corporate "criminal" liability.
	Absent/Missing	**Article 10 – Offences related to infringements of copyright and related rights** 1 Each Party shall adopt such legislative and other measures as may be necessary to	**Missing in AUC.** As a matter of international best practice, especially with the most effective methods of combatting cybercrimes, law enforcement

African Union Convention on Cyber Security and Personal Data Protection (“AUC”)		Budapest Convention on Cybercrime (“BC”)	Comments
		establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system. 2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.	utilizes digital copyright offences as additional criminal conduct to investigate and prosecute several forms of cybercrime (which include crimes such as phishing, electronic fraud, electronic forgery, fraudulent websites and data theft/data breaches). One of the underlying offences in many of these cases tends to be infringement of digital copyright. As a result, several law enforcement units that combat cybercrime are also tasked with combatting digital copyright infringement. It would be impractical and inefficient to combatting cybercrime to disassociate the two. An example of where such joint investigation exists is in the U.S. under the CCIPS. The Sony cyberattack is only one recent example where offences and powers related to cybercrime, data theft/corporate espionage and copyright infringement came together to complement one another. The absence of any provisions relating to intellectual property would constitute a failure to protect the innovation in the 21st century of the African Union Member States, businesses and citizens. The Convention does not call for the creation of a new offence relating to digital copyright infringement. It simply states that if a member state is party to an existing

African Union Convention on Cyber Security and Personal Data Protection ("AUC")		Budapest Convention on Cybercrime ("BC")	Comments
		3 A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.	copyright treaty, it requires that digital copyright infringement be treated as a cybercrime for the reasons mentioned above. Failure to do so would make the AUC an ineffective tool for combatting emerging cybercrime threats in the 21st century.
Article 31: Adapting certain sanctions to Information and Communication Technologies	**1. Criminal Sanctions** a) State Parties shall take the necessary legislative measures to ensure that the offences provided for under this Convention are punishable by effective, proportionate and dissuasive criminal penalties; b) State Parties shall take the necessary legislative measures to ensure that the offences provided for under this Convention are punishable by appropriate penalties under their national legislations; c) State Parties shall take the necessary legislative measures to ensure that a legal person held liable pursuant to the terms of this Convention is punishable by effective, proportionate and dissuasive sanctions, including criminal fines.	**Article 13 – Sanctions and measures** 1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 through 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty. 2 Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.	**AUC largely compatible with BC** This provision is missing the specific language of "deprivation of liberty" which is found in BC, but it may be interpreted to fall under "criminal penalties".
	2. Other criminal sanctions a) State Parties shall take the necessary legislative measures to ensure that in the case of conviction for an offense committed through a digital communication medium, the competent court may hand down additional sanctions;		This provision may be redundant since this has been dealt with already in the AUC.

African Union Convention on Cyber Security and Personal Data Protection ("AUC")		**Budapest Convention on Cybercrime ("BC")**	**Comments**
	b) State Parties shall take the necessary legislative measures to ensure that in the case of conviction for an offence committed through a digital communication medium, the judge may in addition order the mandatory dissemination, at the expense of the convicted person, of an extract of the decision, through the same medium, and according to modalities prescribed by the law of Member States; c) State Parties shall take the necessary legislative measures to ensure that a breach of the confidentiality of data stored in a computer system is punishable by the same penalties as those applicable for breaches of professional secrecy.		Breach of confidential data might be addressed as a civil offence or a violation of regulations or rules of professional conduct and subject to penalties in the form of disciplinary actions/cancellation of licenses etc. Even if they are considered criminal conduct, they ought to be subject to reduced penalties. It appears that this is an attempt to create a yardstick and a floor/minimum threshold to raise the penalties. However, by using the yardstick of professional secrecies, penalties were lowered beneath what is appropriate, particularly in the case of individuals who have stolen data from law firms, government institutions or similar organizations where confidentiality is paramount.
Procedural Law			
	3. Procedural law a) State Parties shall take the necessary legislative measures to ensure that where the data stored in a computer system or in medium where computerized data can be stored in the territory of a State Party, are useful in establishing the truth, the court applied to may carry out a search to access all or part of a computer system through another computer system, where the said	**Article 19 – Search and seizure of stored computer data** 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access: a a computer system or part of it and computer data stored therein; and b a computer-data storage medium in which	**AUC incomplete but compatible with BC.** The aspects of procedural law are dealt with in greater depth than international cooperation. Although this provision does not cover all the aspects of Article 19 of BC, it does deal with the elements of Article 19 in broad

African Union Convention on Cyber Security and Personal Data Protection (“AUC”)		**Budapest Convention on Cybercrime (“BC”)**	**Comments**
	data are accessible from or available to the initial system; b) State Parties shall take the necessary legislative measures to ensure that where the judicial authority in charge of investigation discovers data stored in a computer system that are useful for establishing the truth, but the seizure of the support does not seem to be appropriate, the data as well as all such data as are required to understand them, shall be copied into a computer storage medium that can be seized and sealed, in accordance with the modalities provided for under the legislations of State Parties;	computer data may be stored in its territory. 2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system. 3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to: a seize or similarly secure a computer system or part of it or a computer-data storage medium; b make and retain a copy of those computer data; c maintain the integrity of the relevant stored computer data; d render inaccessible or remove those computer data in the accessed computer system.	terms. Read with the preceding Article (international cooperation), it appears that the AUC mandates the adoption of Article 19. However, to some extent, this provision of the AUC goes beyond Article 19 BC in that powers to extend the search to connected systems is not limited to “its territory”. In principle any computer anywhere in the world could be searched. This provision in b) is missing the element of “similarly access” in BC. As noted in the Explanatory Report to BC, the term ““Search” means to seek, read, inspect or review data. It includes the notion of searching for data and searching of (examining) data. This may lead to a Zoolander situation where law enforcement would be asking, “where are the files”.[17][18][19] The word “access” has a neutral meaning and reflects more accurately computer terminology”.[20] Thus, the AUC appears to have a more limited procedural power relating to search and seizure of stored computer data.

[17] https://goo.gl/5kkRce

[18] https://goo.gl/VnjvK1

[19] http://goo.gl/lujzyu

[20] Paragraph 191 of the Explanatory Report to the BC

African Union Convention on Cyber Security and Personal Data Protection ("AUC")		Budapest Convention on Cybercrime ("BC")	Comments
		4 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2. 5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	
	c) State Parties shall take the necessary legislative measures to ensure that judicial authorities can, for the purposes of investigation or execution of a judicial delegation, carry out the operations provided for under this Convention;		The granting of a general power to judicial authorities as in the AUC is inconsistent with principles of BC, which mandates Parties to enact legislation giving specific powers (i.e. issuance of production orders, warrants for interception of content data etc.) to judicial authorities.
	d) State Parties shall take the necessary legislative measures to ensure that if information needs so require, particularly where there are reasons to believe that the information stored in a computer system are particularly likely to be lost or modified, the investigating judge may **impose an injunction** on any person to preserve and protect the integrity of the data in his/her possession or under his/her control, for a maximum period of two years, in order to ensure the smooth conduct of the investigation. The custodian of the data or	**Article 16 – Expedited preservation of stored computer data** 1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.	**Missing in AUC.** It is important to note that this provision is not an "expedited" power and necessarily requires a judicial order. Granted that it refers to an investigating judge but when translated to a jurisdiction where there are no investigative magistrates this would mean that a judge's warrant would be required. Hence, this does not translate well within all AU member jurisdictions, especially commonwealth countries.

African Union Convention on Cyber Security and Personal Data Protection (“AUC”)		**Budapest Convention on Cybercrime (“BC”)**	**Comments**
	any other person responsible for preserving the data shall be expected to maintain secrecy with regard to the data;	2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person’s possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	Both these aspects undermine the usefulness of such a power and in effect A.16 of the BC is thus, absent from the AUC. This is no more than an injunctive relief or a warrant based power. As mentioned above when dealing with Article 29 BC, this is a serious shortcoming. Further, the use of the terms “injunction” in a commonwealth jurisdiction is a civil restraint that does not necessarily lead to criminal sanctions where one fails to comply. This may be a translation issue, but regardless, a more appropriate term may be used. Preservation for a two year period may be a bit too long even if it is a maximum period and there are judicial oversights. The use of the term “information” rather than “computerized data” appears to be technically incorrect for the purposes of this section.
	e) State Parties shall take the necessary legislative measures to ensure that where information needs so require, the investigating judge can use appropriate technical means to collect or record in real time, data in respect of the contents of specific communications in its territory, transmitted by means of a computer system or compel a service provider, within the	**Article 21 – Interception of content data** 1 Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to: a collect or record through the application of technical means on the territory of that	**AUC compatible with BC but safeguards are missing.**

African Union Convention on Cyber Security and Personal Data Protection (“AUC”)		**Budapest Convention on Cybercrime (“BC”)**	**Comments**
	framework of his/her technical capacities, to collect and record, using the existing technical facilities in its territory or that of State Parties, or provide support and assistance to the competent authorities towards the collection and recording of the said computerized data.	Party, and b compel a service provider, within its existing technical capability: i to collect or record through the application of technical means on the territory of that Party, or ii to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system. 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	
		Section 2 – Procedural law *Title 1 – Common provisions*	**Missing in AUC.**

African Union Convention on Cyber Security and Personal Data Protection (“AUC”)		**Budapest Convention on Cybercrime (“BC”)**	**Comments**
	Absent/Missing	**Article 14 – Scope of procedural provisions** 1 Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings. 2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to: a the criminal offences established in accordance with Articles 2 through 11 of this Convention; b other criminal offences committed by means of a computer system; and c the collection of evidence in electronic form of a criminal offence. 3 a Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20. b Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in	The AUC is missing key procedural powers in the absence of which the investigation and prosecution of cybercrime would be impossible both at a State level and in terms of providing the tools needed to obtain the data that may be requested under requests for mutual assistance and international cooperation. The BC provides detailed procedural powers that are especially required for the purposes of conducting effective investigation and prosecution of cybercrimes and the collection of digital evidence. The absence of such corresponding provisions in the AUC may be remediated if AUC state parties also accede to and ratify the BC, which can act as a patch to the AUC with regards to all procedural powers necessary for an effective framework to combat cybercrime.

African Union Convention on Cyber Security and Personal Data Protection (“AUC”)		**Budapest Convention on Cybercrime (“BC”)**	**Comments**
		Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system: i is being operated for the benefit of a closed group of users, and ii does not employ public communications networks and is not connected with another computer system, whether public or private, that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21.	
	Absent/Missing	**Article 17 – Expedited preservation and partial disclosure of traffic data** 1 Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to: a ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and b ensure the expeditious disclosure to the Party’s competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted. 2 The powers and procedures referred to in	**Missing in AUC.** The preservation and partial disclosure of traffic data is an essential power necessary for investigation of cybercrime. The absence of a provision akin to Article 17 of BC in the AUC shall hinder any effective investigations.

African Union Convention on Cyber Security and Personal Data Protection ("AUC")		Budapest Convention on Cybercrime ("BC")	Comments
		this article shall be subject to Articles 14 and 15.	
	Absent/Missing	*Title 3 – Production order* **Article 18 – Production order** 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order: a a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control. 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15. 3 For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established: a the type of communication service used, the technical provisions taken thereto and the period of service; b the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment	**Missing in AUC.** The AUC is missing a comparable provision to Production Order under BC. The absence of this integral power shall hinder effective investigation and prosecution of cybercrime as well as international cooperation and mutual assistance.

African Union Convention on Cyber Security and Personal Data Protection ("AUC")		Budapest Convention on Cybercrime ("BC")	Comments
		information, available on the basis of the service agreement or arrangement; c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.	
	Absent/Missing	*Title 5 – Real-time collection of computer data* **Article 20 – Real-time collection of traffic data** 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to: a collect or record through the application of technical means on the territory of that Party, and b compel a service provider, within its existing technical capability: i to collect or record through the application of technical means on the territory of that Party; or ii to co-operate and assist the competent authorities in the collection or recording of, traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system. 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its	**Missing in in AUC.** We were unable to find any provision akin to real time collection of traffic data during the course of our review. Such powers are essential to investigation and prosecution of cybercrime and their absence may handicap law enforcement. The absence of this procedural power is inconsistent with BC and international best practices and may tend to impede international cooperation.

African Union Convention on Cyber Security and Personal Data Protection (“AUC”)		**Budapest Convention on Cybercrime (“BC”)**	**Comments**
		territory, through the application of technical means on that territory. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	
Jurisdiction			
	Absent/Missing	**Section 3 – Jurisdiction** **Article 22 – Jurisdiction** 1 Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed: a in its territory; or b on board a ship flying the flag of that Party; or c on board an aircraft registered under the laws of that Party; or d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State. 2 Each Party may reserve the right not to apply or to apply only in specific cases or	**Missing in AUC.** The absence of a clearly defined scope for the offences mandated by the AUC renders unclear the extent of these offences. The unique trans-border nature of cybercrimes requires that the jurisdiction of state parties be specifically defined. In the absence of this, the cybercrime provisions in the AUC may be rendered ineffective.

African Union Convention on Cyber Security and Personal Data Protection (“AUC”)		Budapest Convention on Cybercrime (“BC”)	Comments
		conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof. 3 Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition. 4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law. 5 When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.	