# The Defects of the Draft African Union Convention on the Establishment of a Credible Legal Framework for Cybersecurity

Uchenna Jerome Orji *
*African Centre for Cyber Law and Cybercrime Prevention (ACCP)*
*United Nations, African Institute for the Prevention of Crime and the Treatment of Offenders, Kampala, Uganda.*

* LL.B (Hons.), (University of Nigeria); LL.M (University of Ibadan); Barrister and Solicitor of the Supreme Court of Nigeria; Research Associate at the African Centre for Cyber Law and Cybercrime Prevention (ACCP) of the United Nations, African Institute for the Prevention of Crime and the Treatment of Offenders, Kampala, Uganda. Email: jeromuch@yahoo.com.

**Abstract**

**Within the past decade, Africa has witnessed a phenomenal growth in telecommunications and Internet penetration. Statistical data indicates that Internet users in Africa grew from 4,514,400 million people in 2000 to 167, 335, 676 million people in June 2012[1]. Naturally, the spread of telecommunications technologies and Internet penetration in African states has also raised concerns for cybersecurity at both national and regional levels. At the regional level, the Africa Union Commission and United Nations Economic Commission for Africa has developed a draft regulatory framework on cybersecurity which is known as the Draft Convention for the Establishment of a Credible Legal Framework for Cybersecurity in Africa. The Convention is intended to harmonize the laws of African states on electronic commerce, data protection, cybersecurity promotion and cybercrime control. This paper briefly discuses some of the defects of the Draft Convention with respect to the promotion of cybersecurity and cybercrime control. The paper also offers some suggestions on possible remedies that would enhance the effectiveness of the Draft Convention towards promoting cybersecurity in Africa.**

***Key words: Africa, Computer Emergency Response Teams, Cybersecurity, Double criminality, Economic Commission for Africa, Mutual Legal Assistance, Treaties.***

## I. INTRODUCTION

In recent years, Africa has witnessed a phenomenal growth in telecommunications and Internet penetration. Statistical data indicates that Internet users in Africa grew from 4,514,400 million people in 2000 to 167, 335, 676 million people in June 2012 [2]. This phenomenal growth has been linked to factors such as the liberalization of the telecommunications market in African states, the explosion of mobile and wireless Internet technologies [3], and the increasing availability of broadband systems. With these developments, there has been an increased permeation of Internet technologies in critical economic sectors such as banking and financial services, broadcasting services, aviation services and in several public institutions in Africa. Naturally, the spread of telecommunications technologies and Internet penetration in African states has also raised concerns about cybersecurity at both national and regional levels. Presently, some African states have established cybersecurity laws, while many others are in the process developing cybersecurity initiatives [4]. At the regional level, the Africa Union Commission and United Nations Economic Commission for Africa (UNECA) has developed a draft regulatory framework on cybersecurity which is known as the Draft Convention for the Establishment of a Credible Legal Framework for Cybersecurity in Africa. The Convention is intended to harmonize the laws of African states on electronic commerce, data protection, cybersecurity promotion and cybercrime control. This paper briefly discuses some of the defects of the Draft Convention with respect to the control of cybercrime and the promotion of cybersecurity. The paper also offers some suggestions on possible remedies that would enhance the effectiveness of the Draft Convention towards promoting cybersecurity in Africa.

## II. THE DRAFT CONVENTION FOR THE ESTABLISHMENT OF A CREDIBLE LEGAL FRAMEWORK FOR CYBERSECURITY IN AFRICA

Unlike most regional organizations in other parts of the world, the Africa Union (AU) did not commence the development of any concrete regulatory initiatives on cybersecurity until towards the end of the last decade.[1] A major factor that might have caused the late development of regional cybersecurity initiatives could be traced to the low penetration of Information and Communication Technologies (ICTs) in Africa prior to the recent explosion of wireless technologies within the last decade. One of the first AU statements on the need to promote cybersecurity is found in the *AU Draft Report on a Study of the Harmonization of Telecommunication and Information Communication Technology Policies and Regulation (2008)* [5]. The Draft Report notes *inter alia* that: "emerging questions that needs to be addressed in the converged environment includes the tracing and combating of cybercrime in all its forms (hacking, virus propagation)"[6].

[1] For example, in the Europe, issues relating to cybersecurity have been on the Council of Europe's agenda since 1976. *See* Council of Europe, "Twentieth Conference of Directors of Criminological Research Institutes: Criminological Aspects of Economic Crime" (Strasbourg, 1976). *See* Stein Schjolberg, "The History of Global Harmonization on Cybercrime Legislation – The Road to Geneva" (2008), p.2, available at <http://www.cybercrimelaw.net/documents/cybercrime_history.pdf>[Last visited on 1/10/2013]. *See* Gercke Marco, *Understanding Cybercrime: A Guide for Developing Countries* (ITU: Geneva, 2009) p.95.

The Report also stressed the need to build confidence in the development and use of telecommunications and ICT applications [7] and further emphasized the need for the establishment of a harmonized regional policy and regulatory framework on cybersecurity [8]. On the 5th of November 2009, the AU Ministers in charge of Communication and Information Technologies convened an Extraordinary Session in Johannesburg, Republic of South Africa, where they adopted a set of declarations known as the Oliver Tambo Declaration [9]. The Declaration directed the AU to "jointly develop with the United Nations Economic Commission for Africa, under the framework of the African Information Society Initiative a Convention on cyber legislation based on the Continent's needs and which adheres to the legal and regulatory requirements on electronic transactions, cybersecurity, and personal data protection" [10]. It further recommended AU Member States to adopt the Convention by 2012 [11]. In 2010, the AU Summit explored the theme: "Information and Communication Technologies in Africa: Challenges and Prospects for Development" [12]. Following the summit, the AU Division of Communication and Information produced a report which was adopted by the 14th Ordinary Session of the Assembly of Heads of State and Government of the African Union [13]. The report noted that the United Nations Economic Commission for Africa (UNECA) was addressing cybersecurity within the framework of the African Information Society Initiative (AISI). The AISI advocated a coherent and coordinated regional approach to cybersecurity as well as an enhanced consideration of cybersecurity in national ICT and Information Society strategies and action plans [14]. Accordingly, the UNECA initiative was implemented in cooperation with the AU Commission in order to produce a harmonized legal framework and guidelines on cybercrime, data protection, electronic transactions, e-Signature/certification and cybersecurity [15]. In 2011, the efforts of the AU and UNECA led the development of a draft regulatory framework on cybersecurity known as the Draft Convention for the Establishment of a Credible Legal Framework for Cybersecurity in Africa [16]. The Draft Convention is intended to harmonize the laws of African states on electronic commerce, data protection, cybersecurity promotion and cybercrime control. It lays the foundation for an African Union-wide cybersecurity ethics and enunciates fundamental principles in key areas of cybersecurity. The Draft Convention also defines the objectives for the information society in Africa and seeks to strengthen existing ICT laws in member states and the Regional Economic Communities (RECs) [17]. With respect to cybersecurity, the Draft Convention recognizes that the existence of cybercrime constitutes a real threat to the security of computer networks and the development of the information society in Africa. Accordingly the Convention establishes provisions to promote of cybersecurity and cybercrime control. However, although the Draft Convention represents a landmark attempt to promote cybersecurity in Africa, there are some inherent defects which may hinder its effectiveness as a legal instrument for cybercrime control.

## III. THE PERCEIVED DEFECTS OF THE DRAFT CONVENTION

### *A. The Absence of a Model Legal Framework*

The Draft Convention does not explicitly establish a model legal framework which African countries can adopt. The Convention merely creates directives to guide African states in the establishment of their cybersecurity laws. The language of the Draft Convention does not intend these directives to create an explicit legal framework for the criminalization of cybercrime or for cybersecurity. As such, the adoption and ratification of the Draft Convention by African states will not suffice unless states individually establish cybersecurity laws in accordance with the directives contained in the Convention. It is also not guaranteed that the establishment of such laws will be uniform in order to facilitate regional harmonization. It would be less cumbersome for states if the Draft Convention had explicitly established a model legal framework for states to adopt and ratify into their national laws. Thus, if the Draft Convention had explicitly established a model cybersecurity law, states would not have to commence a fresh process of establishing new laws; they will only have to adopt and modify the model law and than ratify it into their national laws. This option appears to be necessary given that most African states do not have a good record of establishing legal initiatives in record time.[2] Apparently, in

[2] *See e.g.*, the Nigerian Computer Security and Critical Information Infrastructure Protection Bill-Sb 254. [2005]. The Bill was introduced in the Nigerian National Assembly in 2005 and it has remained stagnant since then. The Bill seeks to prohibit cybercrime and establish a legal basis for the protection of computer systems, networks

the absence of such model law on cybersecurity, it may probably take several years for African states to establish cybersecurity laws and also harmonize such laws to achieve effective international cooperation to the widest possible extent.

*B. Mutual Legal Assistance and the Requirement for Dual Criminality (Article III – 1 – 6, p.38 and Article III – 1 – 20)*

Under the Council of Europe Convention on Cybercrime, state parties are allowed to adopt the Convention as a legal basis for extradition proceedings in the absence a mutual legal assistance treaty on extradition. In this regard, article 24(3) of the Council of Europe Convention on Cybercrime provides thus:

> "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" [18].

However, unlike the Council of Europe Convention on Cybercrime, the AU Draft Convention emphasizes the need for states to adopt the principle of double criminality[3] when rendering cross-border assistance on cybersecurity issues. In this regard, the Draft Convention provides that:

> "The cardinal principle of cooperation in the application of the law against cross-border crime reposes on the fact that the laws under which such cooperation is sought by each Member State should be uniform in terms of prohibited conduct and application procedure. Each Member State shall adopt such legal measures as respect the principle of double criminality" [19].

The requirement for dual criminality is also emphasized in article III – 1 – 20 of the Draft Convention which provides that:

> "The cardinal principle of cooperation in the application of the law against cross-border crime reposes on the fact that the laws under which such cooperation is sought by each Member State should be uniform in terms of prohibited conduct and application procedure. Each Member State shall adopt legal measures that respect the principle of double criminality."

However, the problem here is that an African state that may have adopted and ratified the Draft Convention into its national laws may not have a mutual legal assistance treaty with another African state that is also a party to the Convention. In this state of affairs, a request for cross-border legal assistance from one of the states may not be successful. This apparently implies that states parties will individually have to establish mutual legal assistance treaties amongst themselves. As such, each member state of the African Union will have to establish mutual legal assistance treaties with all other states of the Union. This will require each state to engage in tedious negotiations processes which may not always be successful. To prevent this state of affairs, it may be necessary for the Draft Convention to explicitly create provisions enabling African States that do not presently have mutual legal assistances treaties on cybercrime to adopt the Draft Convention as a legal basis for rendering mutual legal assistance in accordance with the principle of double criminality.

*C. The Absence of a Regional African Computer Emergency Response Team (CERT) or a Network Security Agency*

The Draft Convention fails to create a regional Computer Emergency Response Team (CERT) or a regional Network Security Agency to facilitate cybersecurity efforts and also coordinate responses to cybersecurity incidents at the regional level. A regional CERT would

---

and critical information infrastructures in Nigeria. Also for over seven years now the Nigerian Electronic Transactions Bill has also been pending before the National Assembly. The Bill proposes to give electronic documents a functional recognition. *See* Udotai B., "The Growth and Challenges of Information Technology in Law Practice in Nigeria", in Nwosu K., (ed) *Legal Practice Skills & Ethics in Nigeria* (DCON Consulting: Lagos, 2003) pp. 234-233.

[3] "Double criminality" or "Dual criminality" exists where a conduct in issue have been criminalized in the laws of both the State requesting for assistance or extradition and the State from whom such assistance or extradition is requested. Under this principle, an extradition request can only be granted in accordance with an extradition treaty between two countries where both countries have criminalized the criminal conduct for which an extradition request is sought and the crimes are punishable by one year imprisonment or more. *See* ITU High Level Experts Group [HLEG] *ITU Global Cyber-Security Agenda (GCA) High Level Experts Group [HLEG] Global Strategic Report* (ITU: Geneva, 2008) pp.14 and 56. *See The Blacks Law Dictionary* (8th Edition: West Group, 2004) p.537.

have a broader scope of functions and responsibilities than a national CERT or a CERT established by a private organization. A national CERT is usually responsible for coordinating emergency responses to cyber threats affecting national information systems and also establishing best practices relating to use of information systems within a state.[4] However, CERTs that are established by private organizations usually do not have the powers or capacity to deliver such functions on a national scale, because the responsibilities of private CERTs are usually limited to providing to services to clients in the private sector. As such, private CERTs may not provide an effective response to cyber incidents at the national level or in setting regulatory standards for best practices relating to the protection of information systems within a state. On the other hand, a regional CERT may perform the functions of a national CERT at a regional level and also facilitate international cooperation and mutual assistance in the prevention or detection of cyber threats or cybercrime. The Consultative Committee on Cybersecurity which the Draft Convention proposes to establish [20] does not suffice for a regional CERT or a Network Security Agency. This state of affairs will result in the poor coordination of cybersecurity efforts and responses at the regional level. There has been some efforts within the African information security industry to develop a CERT for Africa. For example, African information security experts recently established an industry initiative known as the CERT Africa Project as a continental project with a view to improving information security in the African cyberspace and promoting cooperation through information sharing, human capacity development, awareness creation and the provision of technical facilities for response to cyber threats [21]. There is also another African information security industry CERT initiative which is known as the African Computer Emergency Response Team (AfricaCERT) [22]. The AfricaCERT is meant to function as an international team of trusted African computer incident response teams with a view to achieving cooperation in addressing cybersecurity issues. These industry CERT initiatives have a great potential to enhance private sector participation in African cybersecurity. However, they may not be adequate or effective for the purpose of coordinating public sector and national efforts and responses to cybersecurity at the regional level. Thus, within the framework of the Draft Convention, it is necessary that the African Union may have to establish an institutional framework for cybersecurity which is similar to the European Information Security Agency (ENSIA). The ENSIA was established in 2004 by the European Commission [23] in response to concerns over the some aspects of cybersecurity such as information system security and critical information infrastructure protection. The Agency serves as a center of excellence for member states of the European Union and European institutions in network and information security. It renders advice and recommendations on cybersecurity and also disseminates information on standards for good practices. The Agency also facilitates contacts between EU member states, European institutions, and private business and industry actors [24]. The Agency has also been active in promoting cybersecurity in developing countries.[5]

[4] The responsibilities of a national CERT include (but are not limited to) the following:

(i) Detecting, identifying or monitoring threats to cybersecurity and issuing early warnings of such threats;

(ii) Analyzing and synthesizing incident and vulnerability information disseminated by others, including vendors and technology experts to provide an assessment for interested stakeholders;

(iii) Effectively responding to tackle emergences related threats against computer systems and critical information infrastructures;

(iv) Developing mitigation and response strategies and effecting a coordinated response to the incident;

(v) Providing security analysis of potential vulnerabilities against information systems.

(vi) Sharing data and information about the incident and corresponding responses;

(vii) Tracking and monitoring information to determine trends and long term remediation strategies;

(viii) Establishing trusted communications mechanisms and facilitating communications among stakeholders to share information and address cybersecurity issues; and;

(ix) Publicizing general cybersecurity best practices and guidance for incident response and prevention. *See* ITU Study Group Q.22/1, *Report on Best Practices For A National Approach To Cybersecurity: A Management Framework For Organizing National Cybersecurity Efforts* [Draft] (ITU-D Secretariat: Geneva, January 2008) p. 39/71.

[5] For *e.g.*, the ENISA in conjunction with other international security bodies have supported capacity building and training for CERTs to enhance cybersecurity in African

## IV. CONCLUSION

This paper has briefly discussed some of the perceived defects of the Draft African Union Convention for the Establishment of a Credible Legal Framework for Cybersecurity in Africa. In so doing, the paper also offered some suggestions on how the highlighted defects can be remedied in order to enhance the effectiveness of the Draft Convention towards promoting cybersecurity and cybercrime control in Africa. In June 2012, members of the African Union Expert Group on Cybersecurity from Member States and Regional Economic Communities in Eastern, Southern and Northern Africa met on in Addis Ababa, Ethiopia. One of the aims of that meeting was to present Draft Convention for consideration with members of the Expert Group [25]. Later in September 2012, the members of the African Union Expert Group on Cybersecurity adopted the Draft Convention [26]. This was also followed by its approval by the 22nd Ordinary session of the AU Executive Council in January 2013. The Convention is now awaiting legal validation by the AU Justice Ministers conference in October, 2013 [27] after which it will likely be adopted by the AU Summit in January 2014 and opened for signatures and ratification by AU member states. However, the adoption and ratification of the Convention without a careful consideration of the issues raised in this paper may hinder the effectiveness and success of the Convention. Africa has the opportunity to develop one of most effective regional cybersecurity regimes in the world. This is because, the AU commenced the development of a regulatory framework for cybersecurity later than other regional bodies in other parts of the world, and there are abundant lessons to be learnt from similar initiatives around the world such as the Council of Europe Convention on Cybercrime. Finally, a reconsideration of the Draft Convention is necessary to accommodate the participation of all African states, since it appears that not all African states and stakeholders effectively participated in the consultations that led to its development [28].[6] This is necessary if the Convention would succeed as an effective legal instrument for the harmonization of African cybersecurity laws and the promotion of cybersecurity in Africa.

countries. *See* "Global Security - CERTs in Africa & ENISA", (2010) available at <http://www.prweb.com/ releases/2010/03/prwe b3695284.htm>.[Last visited on 14/1/2012].

[6] *See* "Open Forum to discuss the proposed legal framework for cybersecurity in Africa", (July 26, 2013), available at <http://daucc.wordpress.com/2013/07/26/event-panel-discussion-on-the-draft-african-union-cyber-security-convention/#comment-4> [Last visited on 1/10/2013].

## REFERENCES


[1] *See* Miniwatts Marketing Group, "Internet Usage and Population Statistics for Africa",(June 30, 2012), available at <http://www.internetworldstats.com/stats1.htm>.[Last visited on 1/10/2013].

[2]*See* Miniwatts Marketing Group, "Internet Usage and Population Statistics for Africa",(June 30, 2012), available at <http://www.internetworldstats.com/stats1.htm>.

[3] United Nations Conference on Trade and Development (UNCTAD), "Mobile Telephony in Africa: Cross-Country Comparison", *Information Economy Report 2007-2008* (United Nations: New York, 2008) pp.243 -268.

[4] Uchenna Jerome Orji, *Cybersecurity Law and Regulation* (Wolf Legal Publishers: Netherlands, 2012) pp.401-485.

[5] *See* African Union, *Study on the Harmonization of Telecommunication and Information and Communication Technologies Policies and Regulation in Africa: Draft Report* (African Union, March 2008)p.7, available at <http://www.africaunion.org/root/ua/conferences/2008/mai/ie/1114mai/draft%20report%20study%20on%20telecom%20ict%20policy%2031%20march%2008.pdf.>. [Last visited on 14/1/2012].

[6] African Union, *Study on the Harmonization of Telecommunication and Information and Communication Technologies Policies and Regulation in Africa: Draft Report* (African Union: Addis Ababa, Ethiopia, March, 2008) p.52.

[7] African Union, *Study on the Harmonization of Telecommunication and Information and Communication Technologies Policies and Regulation in Africa: Draft Report* (African Union: Addis Ababa, Ethiopia, March, 2008) p.73.

[8] African Union, Study on the Harmonization of Telecommunication and Information and Communication Technologies Policies and Regulation in Africa: Draft Report (African Union: Addis Ababa, Ethiopia, March, 2008) p.75.

[9] Extra-Ordinary Conference of African Union Ministers in Charge Of Communication and Information Technologies, Oliver Tambo Declaration (Africa Union: Johannesburg, South Africa, 2-5 November, 2009).

[10] Extra-Ordinary Conference of African Union Ministers in Charge Of Communication and

Information Technologies, *Oliver Tambo Declaration* (Africa Union: Johannesburg, South Africa, 2-5 November, 2009), p.4.

[11] Extra-Ordinary Conference of African Union Ministers in Charge Of Communication and Information Technologies, *Oliver Tambo Declaration* (Africa Union: Johannesburg, South Africa, 2-5 November, 2009), p.4.

[12] Division of Communication and Information, *Information and Communication Technologies (ICT) in Africa Challenges and Prospects for Development* – Information Sheet N6 – Cybersecurity (14th African Union Summit: Addis Ababa, Ethiopia, 25 January- 02 February 2010) available at <http://www.africaunion.org/root/au/Conferences/2010/January/summit/informationsheet/TIC%20EN%20AFRIQUE%20-%20FICHE%20D'INFORMATIONS%201%20-%20L'EMERGENCE%20DE%20L'ECONOMIE%20MONDIALE%20DU%20SAVOIR%20ET%20L'AFRIQUE.doc>.[Last visited on 14/1/2012].

[13] Decision Assembly/AU/11(XIV), 14th Ordinary Session of the Assembly of Heads of State and Government of the African Union on Information and Communication Technologies in Africa: Challenges and Prospects for Development, (Africa Union: Addis Ababa, Ethiopia, 1-2 February 2010).

[14] Division of Communication and Information, *Information and Communication Technologies (ICT) in Africa Challenges and Prospects for Development*– Information Sheet N6 – Cybersecurity (14th African Union Summit: Addis Ababa, Ethiopia, 25 January- 02 February 2010).

[15] *See* thenewnewinternet.com, "Proposed Bill Would Curb Cyber Crime in Africa" (7, August, 2011) available at <http://www.thenewnewinternet.com/category/cyber-policy/>.[Last visited on 1/10/2013].

[16] Draft African Union (AU) Convention on the Establishment of a Credible Legal Framework for Cybersecurity in Africa, AU Draft0 010111, Version 01/01.2011, available at <http://au.int/en/sites/default/files/AU%20Convention%20EN.%20(3-9-2012)%20clean_0.pdf>./>.[Last visited on 1/10/2013].

[17] Draft AU Convention on the Establishment of a Credible Legal Framework for Cybersecurity in Africa, p.1.

[18] Article 24(3) of the Council of Europe Convention on Cybercrime.

[19] Draft AU Convention on the Establishment of a Credible Legal Framework for Cybersecurity in Africa, part III, chapter 2 at article III-1-6.

[20] Draft AU Convention on the Establishment of a Credible Legal Framework for Cybersecurity in Africa, part IV, article IV-1(1), p.55.

[21] CERT Africa Project, <http://cert-africa.org/>.[Last visited on 1/10/2013].

[22] AfricaCERT<http://www.africacert.org/home/about-africacert.html>.[Last visited on 1/10/2013].

[23] Regulation (EC) No 460/2004 establishing the European Network and Information Security Agency.

[24] <http://www.enisa.europa.eu/>.[Last visited on 1/10/2013].

[25] *Declaration of Addis Ababa on the Harmonization of Cyber Legislation in Africa* (Economic Commission for Africa: Addis Ababa, 20-22 June 2012), paragraph 10, p.2.

[26] UNECA Press Release, "Draft African Union Convention on Cybersecurity comes to its final stage", available at <http://www1.uneca.org/TabId/3018/Default.aspx?ArticleId=1931>.[Last visited on 1/10/2013].

[27] UNECA Press Release, "ICT Ministers call for harmonized policies and cyber legislations on Cybersecurity", available at <http://www1.uneca.org/ArticleDetail/tabid/3018/ArticleId/1934/ICT-Ministers-call-for-harmonized-policies-and-cyberlegislations-on-Cybersecurity.aspx>. [Last visited on 1/10/2013].

[28] *See* "Open Forum to discuss the proposed legal framework for cybersecurity in Africa", (July 26, 2013), available at <http://daucc.wordpress.com/2013/07/26/event-panel-discussion-on-the-draft-african-union-cyber-security-convention/#comment-4> [Last visited on 1/10/2013].